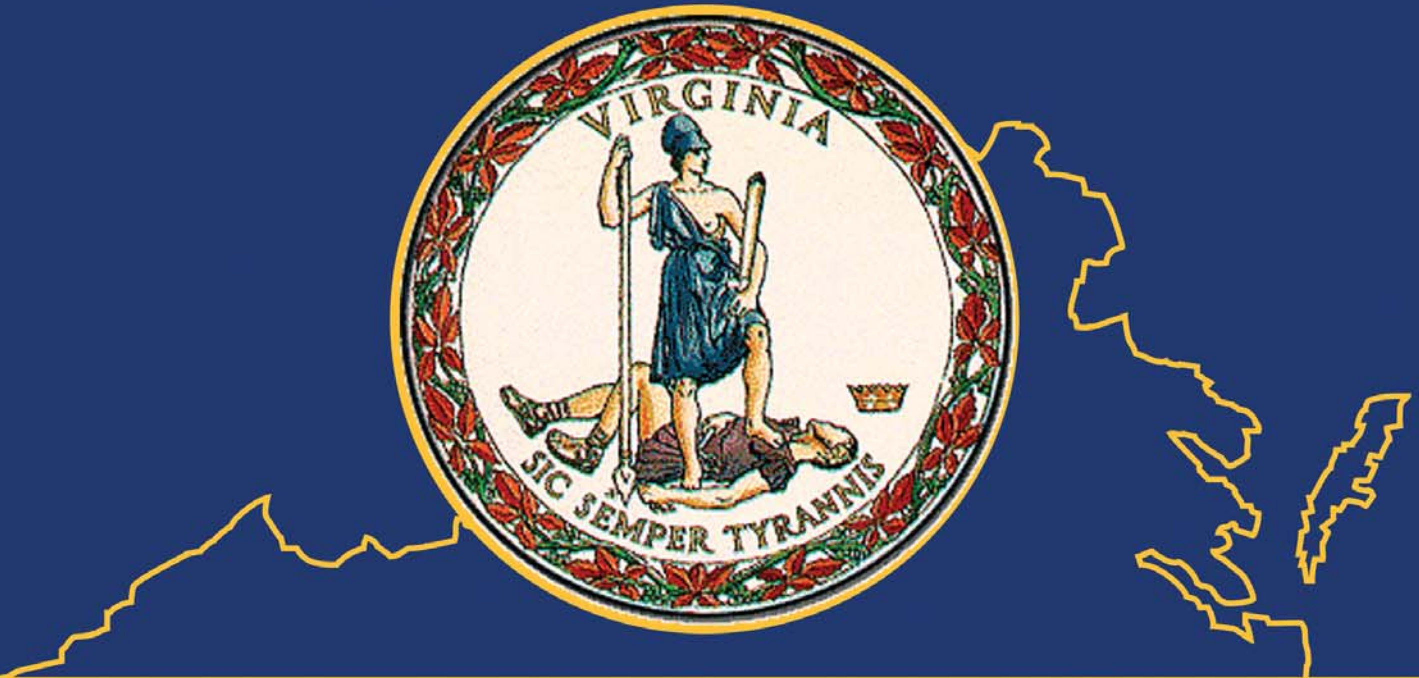
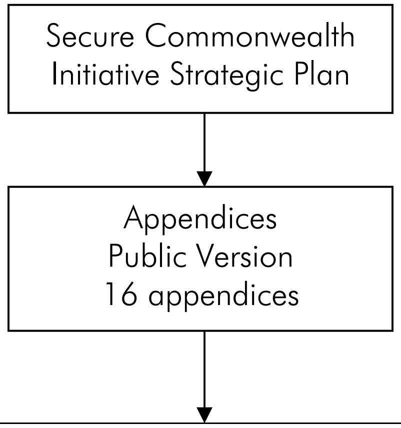


SECURE COMMONWEALTH INITIATIVE STRATEGIC PLAN

APPENDICES


Secure Commonwealth Initiative Strategic Plan
Appendices Public Version 16 appendices

Letter	Name
A	Executive Order 69
B	Secure Commonwealth Panel Members
C	Commonwealth Preparedness Working Group Members
D	Governor's Office of Commonwealth Preparedness and Executive Staff
E	Secure Commonwealth Initiative Working Groups
F	Virginia Citizens Corps
G	Acronyms
H	National and State Guidelines for the Strategic Plan
I	Task Force Strategies ▪ Funding ▪ Intelligence and Information Sharing ▪ Mass Fatalities Management ▪ Performance Measures ▪ Public/Private Cooperation
J	Proceedings of Public Hearings
K	National Strategy for Homeland Security
L	National Strategy to Secure Cyberspace
M	Interim National Infrastructure Protection Plan
N	Interim National Preparedness Goal
O	Recommended Fusion Center Law Enforcement Intelligence Standards
P	2005 National Capital Region Homeland Security Strategic Plan

Appendix A

Executive Order 69
(2004)

APPENDIX A – EXECUTIVE ORDER 69 (2004)

VIRGINIA'S SECURE COMMONWEALTH INITIATIVE

Among the most important responsibilities and profound duties of government at all levels is to provide for the safety and security of its citizens. With this most serious obligation in mind and by virtue of the authority vested in me by Article 5, Sections 1 and 7 of the Constitution of Virginia and by Section 44-146.17 of the Code of Virginia, I hereby establish the Virginia's Secure Commonwealth Initiative. The purpose of this Initiative shall be to implement strategies that enhance the safety and security of the citizens of the Commonwealth. The Initiative shall include, but not be limited to, enhancing the Commonwealth's prevention, preparedness and response and recovery capability for natural disasters and emergencies of all kinds, including terrorist attacks.

SECURE COMMONWEALTH PANEL

To support this Initiative, I hereby establish the Secure Commonwealth Panel (herein called the "Panel") to monitor and assess the implementation of statewide prevention, response and recovery initiatives and where necessary to review, evaluate and make recommendations relating to the emergency preparedness of government at all levels in the Commonwealth. Additionally, the Panel shall facilitate cabinet-level coordination among the various agencies of state government related to emergency preparedness and will facilitate private sector preparedness and communication. The Panel shall deliver to me by December 1, 2005, a comprehensive strategic plan that outlines the status of on-going statewide efforts and recommendations for future activities to manage the physical, economic and societal risks of emergencies and disasters of all kinds, including terrorism.

The Panel shall consist of 20 members. The chairman of the Panel shall be the Assistant to the Governor for Commonwealth Preparedness. Other members of the Panel shall include the Lieutenant Governor; the Attorney General; two members of the House of Delegates; two members of the Senate of Virginia; and the Secretaries of Health and Human Resources, Public Safety, Technology, and Transportation. The Governor shall appoint two local first responders and three local government representatives to the panel. The Governor shall also appoint four additional members from the private sector. Ex officio members may be appointed to the Panel by the Governor at his discretion.

Members of the Panel shall serve without compensation but may receive reimbursement for expenses incurred in the discharge of their official duties upon approval by the Governor's Chief of Staff or his designee. The Panel shall convene, within sixty days of the signing of this order.

The Panel shall prepare quarterly reports for the Governor to keep him apprised of the state's emergency preparedness, response, recovery and prevention efforts. Staff support for the Panel will be provided by the Office of the Governor, the Office of the Secretary of Public Safety, the Office of the Secretary of Health and Human Resources, the Department of State Police, the Department of Emergency Management, the Department of Planning and Budget, and such other executive offices and agencies as may be designated by the Governor. An estimated 500 hours of staff time will be required to support the work of the Panel.

Funding necessary to support the Panel's work will be provided from sources, including both private and appropriated funds, contributed or appropriated for purposes related to the work of the Panel, as authorized by Section 2.2-135(B) of the Code of Virginia. Direct expenditures for the Panel's work are estimated to be $60,000. All or part of the costs incurred by the Panel may be paid, upon my approval, out of the sum sufficient appropriation for Disaster Planning and Operations contained in Item 45 of Chapter 1073, 2000 Virginia Acts of Assembly, or any other funds available for such purpose.

State Agency Plans

I hereby direct all executive branch agency heads to certify to me by June 1, 2004 that they have completed updates and/or development of plans that address continuity of their operations and services, and the security of their customers and employees, in the event of natural or man-made disasters or emergencies, including terrorist attacks. I further direct that all executive branch agencies exercise and test these plans on or before September 1, 2005.

Responsibility for Homeland Security Issues

I hereby designate the Assistant to the Governor for Commonwealth Preparedness as my primary liaison for the U.S. Department of Homeland Security and the Executive Office of the President, Homeland Security Council. He shall be responsible for coordinating, on my behalf, activities as required to promote unity of effort among federal, state, local, private sector and citizen activities related to preparedness and homeland security.

I hereby designate the Secretary of Public Safety as the single point of contact for federal law enforcement agencies regarding homeland security issues and to serve as an alternate liaison to the U.S. Department of Homeland Security and Executive Office of the President, Homeland Security Council if so required.

I hereby designate the Assistant to the Governor for Commonwealth Preparedness to work with appropriate cabinet secretaries to coordinate grants that may be provided to improve preparedness in Virginia communities with the goal of ensuring an integrated enterprise wide approach to prevention and preparedness.

This Executive Order rescinds Executive Order 07 (02). Given under my hand and under the Seal of the Commonwealth of Virginia, this 3rd day of May 2004.

/S/ Mark R. Warner, Governor

Appendix B

Secure Commonwealth Panel Members

APPENDIX B – SECURE COMMONWEALTH PANEL MEMBERS

Jeffrey P. Bialos
Partner, Corporate
Sutherland Asbill & Brennan LLP
McLean, VA

Dr. Vinton G. Cerf
Senior VP, Technology Strategy
MCI
Ashburn, VA

BG (Ret.) Manuel R. Flores
State Director
Selective Service System
Chester, VA

George W. Foresman
Assistant to the Governor
Commonwealth Preparedness
Richmond, VA

Kay C. Goss
Senior Advisor for Homeland Security
Business Continuity and Emergency
Management Services
Electronic Data Systems Corp. (EDS)
Alexandria, VA

The Hon. Katherine K. Hanley
Former Chairman, Fairfax County
Board of Supervisors
Reston, VA

The Hon. Leroy Hassell
Supreme Court Chief Justice
Supreme Court of VA
Richmond, VA

The Hon. Pierce Homer
Secretary of Transportation
Richmond, VA

The Hon. Frank W. Horton
Former Chairman, Russell County
Board of Supervisors
Richlands, VA

The Hon. Janet Howell
VA State Senator
Reston, VA

The Hon. Eugene J. Huang
Secretary of Technology
Richmond, VA

M. Wayne Huggins
Executive Director/Chief Lobbyist
Virginia State Police Association
Richmond, VA

The Hon. Timothy Kaine
Lieutenant Governor
Richmond, VA

The Hon. Judith Williams Jagdmann
Attorney General
Richmond, VA

The Hon. John W. Marshall
Secretary of Public Safety
Richmond, VA

The Hon. Floyd H. Miles, Sr.
Virginia State Delegate
Richmond, VA

The Hon. Brian J. Moran
Virginia State Delegate
Alexandria, VA

Patricia H. Morrissey
Senior National Security Analyst
Science Applications International
Corporation

Potomac Falls, VA

Michael P. Neuhard
Fire Chief, Fairfax County
Fairfax, VA

The Hon. John M. O'Bannon, III
Virginia State Delegate
Richmond, VA

John S. Quilty
Retired Senior Vice President and Director of the Command, Control, Communications and Intelligence (C31) Federally Funded Research and Development Center, the MITRE Corporation
Oakton, VA

The Hon. Beverly J. Sherwood
Virginia State Delegate
Winchester, VA

Suzanne E. Spaulding
Managing Director
The Harbour Group
McLean, VA

Col. Henry W. Stanley, Jr.
Chief of Police, Henrico County
Richmond, VA

Dr. Charles W. Steger
President, Virginia Tech
Blacksburg, VA

The Hon. Kenneth Stolle
Virginia State Senator
Virginia Beach, VA

Regina V. K. Williams
City Manager, Norfolk
Norfolk, VA

Robert W. Woltz, Jr.
President/CEO
Verizon
Richmond, VA

The Hon. Jane H. Woods
Secretary of Health & Human Resources
Richmond, VA

Appendix C

Commonwealth Preparedness Working Group Members

APPENDIX C – COMMONWEALTH PREPAREDNESS WORKING GROUP MEMBERS

George Foresman, Ex-Officio
Assistant to the Governor For
Commonwealth Preparedness

John Marshall, Ex-Officio
Secretary of Public Safety

Bob Newman, Co-Coordinator
Deputy Assistant to the Governor For
Commonwealth Preparedness

Major Mike Bise
Department of Game & Inland Fisheries

LTC Terry A. Bowes
Director, Bureau of Criminal Investigations
Virginia State Police

Brett Burdick
Director, Technological Hazards Division
Department of Emergency Management

Dr. Donald Butts
State Veterinarian
Department of Agriculture and Consumer Services

Janet Clements
Deputy State Coordinator
Department of Emergency Management

Michael M. Cline
State Coordinator
Department of Emergency Management

Colonel Mike Coleman
Department of Military Affairs

Robert Mathieson
Chief Deputy Director
Department of Criminal Justice Services

Jeff Deason
Director of Security Services
Virginia Information Technologies Agency

Marla Graff Decker
Deputy Attorney General
Public Safety & Enforcement Divisio**n**
Office of the Attorney General

Chris Essid
Commonwealth Interoperability Coordinator
Office of the Secretary of Public Safety

Col. W. Steven Flaherty
Superintendent
Virginia State Police

Julian Gilman
Office of Domestic Preparedness Grants
Administrator
Department of Emergency Management

Buddy Hyde
Executive Director
Department of Fire Programs

Major Michael A. Jones
Assistant Chief of Police
Virginia Capitol Police

Dr. Lisa G. Kaplowitz
Deputy Commissioner for Emergency
Preparedness and Response
Department of Health

Paul E. Lubic, Jr.
Associate Director for Policy, Practice and
Architecture
Virginia Information Technologies Agency

Colonel George Mason
Chief of Police
Capitol Police

Robert Mauskapf
Statewide Planning Coordinator
Department of Health

Constance McGeorge
Special Assistant
Office of Commonwealth Preparedness

John Miller
Chief, Resource Protection
Department of Forestry

Steve Mondul
State Director, Security and Emergency Mgmt.
Department of Transportation

Michael Murphy
Director, Division of Environmental Enhancement
Department of Environmental Quality

Janet Queisser
Emergency Planning and Response
Coordinator
Department of Environmental Quality

Charlie Sledd
Program Development Director
Department of Game and Inland Fisheries

Fred Vincent
Commonwealth Security Coordinator
Department of Emergency Management

Tom Wilcox
Department of Game & Inland Fisheries

Appendix D

Governor's Office of Commonwealth Preparedness and Executive Staff

APPENDIX D – GOVERNOR'S OFFICE OF COMMONWEALTH PREPAREDNESS AND EXECUTIVE STAFF

The Office of Commonwealth Preparedness was first created by Governor Warner's Executive Order 07 (02), continued by Executive Order 69 (04), and is responsible for translating vision into reality by synchronizing actions, both public and private, and by insuring that financial resources are being expended on shared statewide preparedness goals. The Office's role is one of policy, coordination, leadership and resource allocation between agencies of state government entrusted with public safety and security responsibilities. The Office serves as a direct liaison between the Governor and Virginia's local governments and first responders on issues of emergency preparedness. It helps educate the public on homeland security issues and responds to inquiries for support and guidance. The Office of Commonwealth Preparedness is the single point of contact in Virginia with the Department of Homeland Security. The Office is leading the effort to secure additional federal funding for preparedness initiatives, as Virginia's unique geographic location - home to the world's largest navel base, a hub for Internet traffic, neighbor to the nation's capitol and backup location for federal operations – places the Commonwealth high on the list of potential terrorist targets.

The Assistant to the Governor for Commonwealth Preparedness serves in a cabinet level position and heads the Office of Commonwealth Preparedness. This new office was established by Governor Warner by Executive Order 07 (02) to lead Virginia's preparedness effort and to coordinate Virginia's security in the fight against terrorism and was continued by Executive Order 69 (04). The Office is charged with the responsibility to work with Virginia's congressional delegation and the President's administration in obtaining additional federal resources for security.

GEORGE W. FORESMAN
ASSISTANT TO THE GOVERNOR FOR COMMONWEALTH PREPAREDNESS

George W. Foresman serves Virginia's citizens and Governor Mark R. Warner as Assistant to the Governor for Commonwealth Preparedness. In this capacity he is the principal advisor and overall coordinator for homeland security, preparedness, and relations with military commands and installations throughout Virginia.

Foresman chairs the Secure Commonwealth Panel and leads the Governor's related initiative responsible for strengthening Virginia's security and preparedness for emergencies and disasters of all kinds, including terrorism. He serves as Virginia's principal liaison with the White House, Congress, U.S. Department of Homeland Security, and other federal entities to coordinate homeland security policy and programs as well as obtaining resources.

Maintaining a productive relationship with the Department of Defense and Armed Services remains a priority for Governor Warner. Foresman serves as the Governor's direct Cabinet level liaison with top defense and military officials, commands and installations. He is the vice-chair of the Virginia Military Advisory Council which serves to foster civil-military communication and pro-military policies across Virginia. Foresman also provides oversight of the Commonwealth's activities relative to federal base realignment and closure process.

Foresman is a nationally recognized expert on emergency preparedness and homeland security. He was a member and vice-chair of the Advisory Panel to Assess Domestic Response Capabilities Involving Terrorism, established by Congress in 1998 to evaluate America's readiness for terrorism. The Panel delivered five annual reports to the Congress and President before completing its work in December 2003. More than 125 of the Panel's 144 recommendations have been adopted in part or whole. He frequently is solicited for consultation on national policy issues.

A native of Lexington, Virginia, Foresman joined state government in 1985. He possesses more than 20 years of experience in emergency management, law enforcement, fire and emergency medical service organizations ranging from operations to executive level leadership.

Mr. Foresman is a graduate of the Virginia Military Institute as well as the Virginia Executive Institute.

ROBERT B. NEWMAN, JR.
DEPUTY ASSISTANT TO THE GOVERNOR FOR COMMONWEALTH PREPAREDNESS

Governor Mark Warner appointed Mr. Newman on July 1, 2004. A Brigadier General in the Air National Guard, he is the Vice Director for Operations, Logistics, and Engineering at the United States Joint Forces Command in Norfolk. Following the attacks of September 11, 2001 he was called to active duty and served at the National Guard Bureau in Washington DC. He headed the Domestic Operations Division that was responsible for the development of a critical infrastructure protection program for the fifty-four states and territories.

Newman has been associated with the financial services industry since 1981. He was worked for national and regional brokerage firms specializing in institutional fixed income sales.

Newman is a graduate of the Virginia Military Institute, where he received a Bachelor of Arts degree in Economics, and of Webster University, where he received a Master of Arts degree in Management and Public Administration.

Appendix E

Secure Commonwealth Initiative Working Groups

APPENDIX E – SECURE COMMONWEALTH INITIATIVE WORKING GROUPS

VIRGINIA MILITARY ADVISORY COUNCIL

The Virginia Military Advisory Council plays a parallel role to the Panel with the active duty military bases located in Virginia, which are vital to America's security defenses and of great importance to the economy of the Commonwealth. The role of the Council is to foster coordination, communication and cooperation between the Commonwealth and the leadership of the U.S. Armed Forces stationed in the Commonwealth. The Council is charged with encouraging regular communication regarding continued military facility viability; the exploration of privatization opportunities; and issues affecting preparedness, public safety and security. Section 2.2-2666.1 of the Code of Virginia established the Council, which is composed of 25 members.

COMMONWEALTH PREPAREDNESS WORKING GROUP

The Commonwealth Preparedness Working Group is composed of key representatives of state agencies involved in preparedness and homeland security related operations. Members of the Working Group function as a team to support the Panel and coordinate state agency action during threat situations, incidents or challenges facing Virginia. They also propose projects for funding and work hard to break down the old "stovepipe" structure of government. The team meets regularly to coordinate and assess the state's preparedness and readiness. The Working Group is comprised of representatives from the Secretary of Public Safety, Office of Commonwealth Preparedness, Virginia State Police, Department of Emergency Management, Department of Agriculture and Consumer Services, Department of Military Affairs, Department of Fire Programs, Department of Health, Department of Transportation, Capitol Police and Secretary of Commerce and Trade.

Appendix F

Virginia Citizen Corps

APPENDIX F – VIRGINIA CITIZEN CORPS

Virginia Citizen Corps Program provides an opportunity for citizens of the Commonwealth to take an active role in the provision of security and preparedness in their communities. Local Citizen Corps Councils in every region of the state bring emergency management experts to the table with citizen volunteers to work together to make communities more prepared and secure for emergencies, hazards, threats and disasters of all kinds.

Forty-eight local and six regional Citizen Corps Councils serve the Commonwealth. The Councils coordinate outreach and preparedness programs for 75% of Virginia's population, providing community based training and volunteer activities that assist and support the first responder and public safety communities. Local programs serve more than 70 localities.

Local Citizen Corps programs in Virginia provide outreach, education, training and exercise opportunities to teach citizens of the Commonwealth skills that can be used year-round, in times of emergencies, or during disasters. Citizens learn to conduct damage assessments, provide shelter services, safely operate equipment such as chain saws, support staff in local emergency operation centers, set up and operate amateur radio communication and command centers, make individual and neighborhood preparedness plans, assembly preparedness kits, teach preparedness skills and identify and report criminal and terrorist activities.

Local Citizen Corps Councils provide the oversight for these activities in Virginia. Membership on these local councils must mirror the make-up of the community. Each local council must have representation from first responders, law enforcement, emergency management, local government, health, volunteer community, faith-based community, public utilities, the private sector and citizens.

The five core Citizen Corps programs are Community Emergency Response Team Training (CERT), Fire Corps, Medical Reserve Corps, Neighborhood Watch and Volunteers in Police Service.

More than 3,500 citizens are CERT trained. There are 15 Virginia Medical Reserve Corps programs. There are 4,794 Neighborhood Watch groups in Virginia with an average of 66 households participating in each group. And there are more than 30 local Volunteers in Police Service programs. The Fire Corps is Virginia's newest Citizen Corps program; it is being established under the direction of the Virginia Department of Fire Programs.

Appendix G

Acronyms

APPENDIX G – ACRONYMS

BRAC	Base Realignment and Closure
CBRNE	Chemical, Biological, Radiological, Nuclear, Explosives
CCP	Citizen Corps Program
CERT	Community Emergency Response Team
CIPWG	Critical Infrastructure Protection Working Group
COG	Continuity of Government
COOP	Continuity of Operations Plan
DCJS	Department of Criminal Justice Services
DHS	Department of Homeland Security
DOAV	Virginia Department of Aviation
DOD	Department of Defense
EAS	Emergency Alert System
EMAP	Emergency Management Accredited Program
EMS	Emergency Medical Service
EOC	Emergency Operations Center
GIS	Geographic Information System
HSGP	Homeland Security Grant Program
JIC	Joint Information Center
JLARC	Joint Legislative Audit and Review Commission
LETPP	Law Enforcement Terrorism Prevention Program
NCR	National Capitol Region
OCP	Office of Commonwealth Preparedness
OEMS	Office of Emergency Medical Services
ODP	Office of Domestic Preparedness
PIO	Public Information Officer
SHSP	State Homeland Security Program
SIEC	State Interoperability Executive Committee
SWAN	Statewide Alert Network
TSA	Transportation Security Administration
UASI	Urban Area Security Initiative
VBMP	Virginia Base Mapping Program
VCOMB	Virginia Commission on Military Bases
VMAC	Virginia Military Advisory Council
VDACS	Virginia Department of Agriculture and Consumer Services
VDEM	Virginia Department of Emergency Management
VDFP	Virginia Department of Fire Programs
VDH	Virginia Department of Health
VDOE	Virginia Department of Education

VDOT	Virginia Department of Transportation
VEOC	Virginia Emergency Operations Center
VERT	Virginia Emergency Response Team
VGIN	Virginia Geographic Information Network Division
VISWG	Virginia Information Sharing Working Group
VITA	Virginia Information Technologies Agency
VPA	Virginia Port Authority
VR3	Virginia Readiness, Response and Recovery GIS
VSP	Virginia State Police

Appendix H

National and State Guidelines for the Strategic Plan

APPENDIX H – NATIONAL AND STATE GUIDELINES FOR THE STRATEGIC PLAN

The Secure Commonwealth Panel adopted this five-year comprehensive all-hazards preparedness strategy to set forth the Commonwealth's vision and priorities for ensuring a secure and prepared Commonwealth.

It is the intent of the Commonwealth to act in alignment with the National Preparedness Goal and seven National Priorities:

1. Implement the National Incident Management System and National Response Plan.
2. Expand Regional Collaboration.
3. Implement the National Infrastructure Protection Plan.
4. Strengthen Information Sharing and Collaboration Capabilities.
5. Strengthen Interoperable Communications Capabilities.
6. Strengthen CBRNE Detection, Response, and Decontamination Capabilities.
7. Strengthen Medical Surge and Mass Prophylaxis Capabilities.

The Secure Commonwealth Initiative's Strategic Plan is also aligned with Virginia's statewide long-term objectives as articulated by the Council on Virginia's Future:

1. Be recognized as the best managed state in the nation.
2. Be a national leader in the preservation and enhancement of our economy.
3. Engage and inform citizens to ensure we serve their interests.
4. Elevate the levels of educational preparedness and attainment of our citizens.
5. Inspire and support Virginians toward healthy lives and strong and resilient families.
6. Protect, conserve, and wisely develop our natural, historical, and cultural resources.
7. Protect the public's safety and security, ensuring a fair and effective system of justice and providing a prepared response to emergencies and disasters of all kinds.
8. Ensure that Virginia has a transportation system that is safe.

Appendix I

Task Force Strategies

Appendix I-1

Funding Task Force of the Secure Commonwealth Panel

Recommendations to The Secure Commonwealth Panel And The Office of the Governor – Commonwealth Preparedness

May 10, 2005

Table of Contents

Members

The Honorable Katherine K. Hanley, Chair
Former Chairman, Fairfax County Board of Supervisors

The Honorable Frank W. Horton
Former Chairman, Russell County Board of Supervisors

The Honorable Barry Green
Deputy Secretary, Secretary of Public Safety

Regina V.K. Williams
City Manager, Norfolk

Lisa G. Kaplowitz, Ph.D.
Deputy Commissioner for Emergency Preparedness and Response
Virginia Department of Health

James W. Keck
Deputy State Coordinator
Virginia Department of Emergency Management

Philip A. Broadfoot
Police Chief
Danville, VA

R. Steven Best
Fire Chief
Chesapeake, VA

Robert Mathieson
Chief Deputy Director
Department of Criminal Justice Services

Julian Gilman
Virginia Department of Emergency Management

Charles E. Jett
Sherriff
Stafford, VA

James D. Campbell, CAE
Executive Director, Virginia Association of Counties

Malvern R. “Rudy” Butler
1st Vice President, Virginia Association of Counties

Janet Areson
Virginia Municipal League

Ron Carlee
Emergency Services Director and County Manager
Arlington, VA

John C. McGehee
Assistant Administrator
Verona, VA

William R. Nelson, Ph.D.
Public Health Officer/Health Director
Chesterfield, VA

John Crooks
Budget Analyst
Department of Planning and Budget

Pete Sommer
Emergency Management Coordinator
Hampton, VA

Carol Scarton
Purchasing Agent
Prince William, VA

Brent Robertson
Director of Management and Budget
Roanoke County, VA

Suzanne Simmons
Citizen Corps Program Manager
Virginia Department of Emergency Management

Arlene K. Ney
Accountant IV, Finance/Comptroller's Office
Virginia Beach, VA

Meredith K. Ching
Management and Budget Analyst, Management Services
Virginia Beach, VA

Introduction

The challenge for the Funding Task Force, as reflected in its mission statement, was to find ways to help localities be efficient and effective in funding and implementing appropriate homeland security projects in a timely manner, and to be proactive in responding to possible future Federal rules changes.

The task force held three teleconferences to discuss issues surrounding current processes and to make recommendations that would improve the process in the future. Because task force members represented a wide range of perspectives, a consensus developed that recommendations must include enough flexibility to meet a variety of needs.

Thank you to all the task force members, with special thanks to Barry Green and the Formula Subcommittee.

Kate Hanley, Chair

Mission of the Task Force

Examine the methodologies for funding localities and determine what is a reasonable approach for the future, with potential decreases in Federal funding likely. Ensure a funding approach that will put taxpayer dollars to the best use for securing all localities in Virginia.

Policy Issues

- *Determine how the Commonwealth should approach dispersal of homeland security funding in a way that will increase preparedness and security statewide*
- *Determine how the Commonwealth and its localities can adapt to likely decreases in Federal homeland security funding*
- *Develop and evaluate the funding process on both the State and local levels*

Recommendations

I. Policy

Structure and Strategy

The Commonwealth as a whole and the individual entities within it need to develop long-term plans for homeland security funding.

Issue 1 - Localities should have long-term homeland security plans and a funding strategy to implement those plans.

Recommendations

1. Each locality should adopt a five-year plan that is compatible with the Secure Commonwealth Panel's strategic plan.

2. The local plans should be updated each year to reflect goals that have been met and new goals and performance measures.

Issue 2 - What should local homeland security funding plans contain and how will they fit into the Commonwealth's strategic plan?

Recommendation

The task force recommends that the Secure Commonwealth Panel, as a whole, address this issue because it is broader than funding.

Issue 3 - If the Federal government requires a regional approach to funding homeland security projects, how will the Commonwealth implement that requirement?

Recommendation

Rather than have the Commonwealth define specific regions, localities are encouraged to develop multijurisdictional projects. This will allow different combinations of localities to make proposals addressing a variety of issues.

The Commonwealth's Ability to Adapt to Federal Issues

The Commonwealth should be prepared for possible decreases in Federal homeland security funding.

Issue 1 - How can localities best prepare for possible decreases in Federal funding?

Recommendation

Each locality spending plan should include proposed items to be purchased (whether goods or services) and should include a prioritization. A prioritized purchase list will better enable localities to identify alternate goods or services to purchase if funding received is less than identified as needed.

II. Process

Efficiency

It is vital that the Commonwealth disperse Federal homeland security funds to localities in a clear award letter and in a timely manner. In turn, localities should have a plan for the funds, be prepared to spend them, and report back to the State on how the funds were used to increase their security and preparedness.

Issue 1 - Localities do not know how much Federal homeland security money they will receive until after they have passed their budgets.

Recommendations

1. The Commonwealth should publish the homeland security grant amounts as soon as it receives them, so that localities can calculate the approximate amount of funding they will receive when preparing when their budgets.

2. Local governing bodies must meet to approve changes to their budgets. This is often necessary regarding homeland security funds, as these are dispersed after localities pass their budgets. Thus, there should be a 60-day turnaround between notification of the amount of funding localities will receive and grant proposal submissions. This timeframe will give local governing bodies in the Commonwealth time to approve changes to their budgets.

3. In order to provide localities with a guaranteed amount of funding for security and preparedness programs, the Commonwealth could appropriate $10,000 in State funding to localities annually. Federal funding, on a grant basis, would supplement local initiatives.

Issue 2 - Localities are required to spend homeland security funds within a certain time period or the State will reallocate the unspent money. The funding guidelines and deadlines should be made clear to localities up front.

Recommendations

1. It is important to continue to deal with localities on a case-by-case basis because each locality is different and may require the State to provide special assistance or grant exceptions.

2. Each locality's funding request should reflect the goals contained in its long-term funding plan.

III. Implementation

Funding Formula

The Commonwealth is charged with dispersing Federal homeland security funds to localities. Of the homeland security funds, 80% goes to localities and 20% to State agencies. A clear formula for funding dispersal will allow localities to begin to plan ahead based on the amount of funding they anticipate receiving.

Issue 1 - The funding formula needs to be revamped based on evolving Federal criteria, as well as on what the Commonwealth has learned from the past funding cycles.

Recommendations

1. Identify the amount of the 80% local share of the total applicable Federal grant for the year. This must be done in a timely manner.

2. Each locality (134 in total) will receive a base amount of $10,000, off the top of the 80% share.

3. Of the remaining amount:
   - 35% will be distributed based on population
   - 35% will be distributed based on risk
   - 30% will be awarded through a competitive grant process

4. Competitive grants will be capped at:
   - $100,000 for a single locality
   - $250,000 for a multijurisdictional grant including two–three localities
   - $350,000 for a multijurisdictional grant including four or more localities

5. In assessing competitive grant proposals, preference will be given to multijurisdictional solutions, and to proposals that involve promising technology or concepts that may be piloted to determine appropriateness for statewide application.

Issue 2 - What is required of the Commonwealth to implement this new funding plan?

Recommendations

1. The Secure Commonwealth Panel must complete the statewide strategic plan and require localities to have plans that are consistent with the statewide plan

2. The Secure risk criteria Commonwealth Panel must develop risk criteria and decide how to assign scores to localities based on such criteria

3. The Secure Commonwealth Panel can recommend the appointment of members and staff to assess competitive grant proposals

Conclusion

In the process of making its recommendations, the task force identified several issues that are beyond the scope of the funding process and are therefore more appropriately addressed by the Panel as a whole.

The Funding Task Force recommends that each locality have a long-term (possibly five years) homeland security plan that identifies projects to be undertaken, and that is consistent with the State strategic plan. What those plans should include and how they are developed and reviewed is a broader matter than funding, and should be considered by the entire Panel.

The task force recommends that risk should be a factor in evaluating grant applications. Therefore, criteria for determining and evaluating risk need to be established. Again, this is a task beyond the charge to the task force.

In conclusion, the task force found that a funding process that is transparent at the beginning of a funding cycle, that includes multiyear plans, and that is flexible enough to recognize the diversity of needs in the Commonwealth will be more efficient and effective for both the State and its localities, thereby improving the safety and security of Virginia's citizens.

Appendix I-2

Intelligence and Information Sharing Task Force of the Secure Commonwealth Panel

Recommendations to The Secure Commonwealth Panel And The Office of the Governor – Commonwealth Preparedness

May 10, 2005

Table Of Contents

Members

Suzanne E. Spaulding, Chair
Managing Director, The Harbour Group LLC

The Honorable John W. Marshall
Secretary of Public Safety

Robert B. Newman, Jr.
Deputy Assistant to the Governor,
Office of Commonwealth Preparedness

Dr. Lisa G. Kaplowitz
Deputy Commissioner for Emergency Preparedness and Response,
Virginia Department of Health

Steven M. Mondul
State Director, Security & Emergency Management,
Department of Transportation

Michael M. Cline
State Coordinator, Virginia Department of Emergency Management

Colonel W. Steve Flaherty
Superintendent, Virginia State Police

Michael P. Neuhard
Fire Chief, Fairfax County Fire & Rescue Dept

Colonel Henry W. Stanley, Jr.
Chief of Police, Henrico County Police

Colonel Michael J. Coleman
Director of Plans, Operations & Training,
Department of Military Affairs

Patricia H. M. Morrissey
Senior National Security Analyst, Hicks & Associates, Science Applications International Corp (SAIC)

William H. Parrish
Associate Professor, L. Douglas Wilder School of Government and Public Affairs,
Virginia Commonwealth University

John S. Quilty
Retired, Senior Vice President and Director,
MITRE Corporation

Introduction

Mission of the Task Force

Review strategic intelligence and information sharing among the various levels and agencies of government and address theses issues from a policy and operations standpoint, based on what is in place and what the Commonwealth should do in the future.

Process

The task force began in the same way that an effective intelligence cycle begins, by identifying information requirements for terrorism preparedness and response in the Commonwealth. This was followed by a discussion of how various State and local entities can contribute to efforts to meet the identified information needs. Key to the discussion was recognition that virtually every player is both a collector and a consumer of relevant information. Finally, the task force focused most of its effort on identifying specific challenges to meeting the overall goal of enhancing Commonwealth preparedness through more robust and effective information sharing. The task force developed recommendations for addressing each challenge or issue identified. In all of these discussions, the task force was mindful of the extensive collaborative structures and processes that are already in place and working well throughout the State.

Guiding Principles

The task force recognized that the primary mechanism for intelligence and information sharing will be the new Fusion Center. However, it was also understood that information sharing must extend beyond the Center—through virtual sharing structures, training, and protocols at all levels of government and with the private sector—so that a culture of appropriate and effective sharing becomes ingrained.

Using the statutory authorization for the establishment of the Fusion Center as a guide to legislative and executive intent with regard to information sharing, the task force recommendations reflect a broad, interagency focus rather than the law enforcement focus that often characterizes other State fusion centers and intelligence and information sharing efforts. Having said that, national guidance documents developed for law enforcement information sharing efforts provided useful checklists for the task force as it identified issues and developed proposals.

Similarly, the task force understood that the goal is to enhance the sharing of all relevant information, not just that typically labeled as "intelligence." There are many different ways to define "intelligence." This can lead to confusion since readers may be unclear about which definition applies in any given context. Thus, the task force uses the term *"information" unless specifically referring to classified information provided by Federal intelligence agencies.*

Nevertheless, what is typically referred to as the "intelligence cycle" can serve as a useful overall guide for any organization or level of governments attempting to ensure it has the information necessary to guide decisionmaking. The process begins with identifying information requirements, followed by an evaluation of how those requirements are currently being met, where there are gaps, and how those gaps can be filled through additional or improved information gathering and collection efforts. The next step is ensuring the information, once gathered, is disseminated to those who need it. This includes analysts who can put the information in context as well as ultimate end-users. These "consumers" should then evaluate the information and provide feedback on the requirements identification process, assessing how well the information meets the needs of users and what gaps still exist.

The entire process must be guided by clear policy directives, implemented by an appropriate governance structure, informed by protocols and interagency agreements, and inculcated through appropriate training. The need to protect civil liberties and sensitive information must be fully considered at every level of the process. Sensitive information includes information that raises privacy concerns, law enforcement sensitive information, and information governed by HIPPA and other health and medical requirements.

Finally, the task force recognized that the Commonwealth's information sharing must take into consideration Federal initiatives, capabilities, and requirements.

These are the key issues and challenges that informed the task force as it formulated the recommendations outlined below.

Recommendations

I. Policy

Civil Liberty Protections

Terrorists seek to destroy lives and our way of life. The homeland security imperative is to deny them both of these objectives. Thus, civil liberty protections must be an inherent aspect of the Commonwealth's enhanced information sharing initiatives.

Issue 1 - Who should be in charge of overseeing the protection of civil liberties in the Commonwealth in the context of these intelligence and information sharing initiatives?

Recommendation

Ultimately, the responsibility to preserve civil liberties cuts across all agencies and entities involved and comes together at the level of the chief executive. Thus, the Governor's Office of Commonwealth Preparedness and/or the Governor's policy office should be responsible for ensuring that there is an independent arbiter to safeguard the civil liberties and privacy of the Commonwealth's citizens throughout the process of information collection, analysis, and dissemination. Appropriate consideration should be given to including nongovernmental representatives as part of this important oversight function.

All-Hazards Approach

While the focus of the task force was terrorism-related information, the long-term goal of the fusion process is to manage all risks to the Commonwealth, not just terrorist threats.

Issue 1 - How can the Commonwealth ensure the information sharing process can ultimately serve preparedness needs beyond the terrorist threat?

Recommendation

The Office of Commonwealth Preparedness should be tasked with ensuring local governments and first responders are included in discussions on Commonwealth security and preparedness and in the intelligence and information sharing process, as well as in identifying new partners.

II. Governance

It is essential to effective governance of the information sharing process that roles and responsibilities be clearly established. Responsibility for ensuring Commonwealth preparedness with respect to the terrorist threat falls upon the Governor, who has designated the Office of Commonwealth Preparedness as the primary executive agent in this regard. Responsibility for implementation of this authority is spread across many departments, agencies, and offices at the State and local level. The private sector also has preparedness obligations. In addition, the legislature provides statutory authority and funding for effective implementation of these fusion efforts.

Issue 1 - How does the Commonwealth ensure effective management of this collaborative process?

Recommendations

1. A governance structure that includes broad representation from all appropriate entities at the State and local level, as well as from the private sector, should be established for the information sharing process. This structure should report to the Governor, through the Office of Commonwealth Preparedness.

2. The Virginia Fusion Center is a key element of the information sharing process. As such, it should, consistent with the authorizing legislation, be operated by the Department of State Police in cooperation with the Department of Emergency Management and other State and local agencies and private organizations, pursuant to the guidance and direction of the Governor, on behalf of this collaborative governance structure. The director of the Fusion Center should report directly to the head of this governance structure, as designated by the Governor.[1]

Issue 2 - The legislature must be given the information it needs to better understand the requirements associated with requests for resources to enhance the security and preparedness of the Commonwealth.

Recommendations

A(v)[1] Section 52-47 of the Code of Virginia was enacted by the General Assembly in 2005 to establish Virginia's Intelligence Fusion Center. That section states: "*The Governor shall establish, organize, equip, staff, and maintain a multiagency intelligence fusion center to receive and integrate terrorist-related intelligence and information. The Department of State Police shall operate the facility, as directed by the Governor and in cooperation with the Department of Emergency Management and other such state and local agencies and private organizations as the Governor may deem appropriate. The fusion center shall collect, analyze, disseminate, and maintain such information to support local, state, and federal law-enforcement agencies, and other governmental agencies and private organizations in preventing, preparing for, responding to, and recovering from any possible or actual terrorist attack.*"

1. Members of the General Assembly should be provided with intelligence assessments that will help them fully appreciate potential threats and security issues confronting the Commonwealth. The Intelligence Fusion Center should prepare an annual Intelligence Assessment that is drawn from national intelligence assessments and estimates, Department of Homeland Security and Federal Bureau of Investigation Advisories and Alerts, and other sources of intelligence and information including "Open Source" reporting and local and State information and intelligence that can help particularize the Federal intelligence to Virginia. The Intelligence Assessment should be prepared up to the Sensitive but Unclassified level. Prior to its release the Assistant to the Governor for Commonwealth Preparedness will coordinate annual review and approval of the Commonwealth's Annual Intelligence Assessment with the Secretary of Public Safety, Adjutant General, Superintendent of Virginia State Police, Coordinator of Emergency Management, Commissioner of Health, and others as needed. Upon approval of the Intelligence Assessment, the Director of the Intelligence Fusion Center should brief designated members of the Governor's Cabinet and key leaders in the General Assembly, including designated Committee Chairs and the Speaker of the House. This briefing should be provided within the first three days of the General Assembly's annual session.

2. Additionally, the Intelligence Fusion Center should prepare Sensitive but Unclassified Quarterly Intelligence Summaries that will be made available to designated Cabinet level officials and designated members of the General Assembly.

III. Structure and Strategy

There is an evident need to share information horizontally across agencies and departments, vertically between the levels of government, and between the government and the private sector. The Fusion Center will provide the primary structure for the information sharing process.

Issue 1 - How can the Commonwealth best ensure the Fusion Center succeeds in improving information flow between agencies and maximizing their input into the fusion process?

Recommendations

1. At the State level, the Fusion Center concept should be designed to facilitate effective information sharing by ensuring individuals representing the key players can come together in a common facility and by providing the nexus for an ongoing intelligence exchange. While this may not eliminate all stovepiping and cannot force sharing at the Federal and local levels, it does provide a mechanism for fusing information at the

State level and may have some impact on forging a new culture. Thus, the Fusion Center will be an ongoing effort to facilitate sharing of information and intelligence.

2. By the time the Fusion Center is operational, each agency should have identified a representative to the Center. This individual will obtain relevant mission-critical information as it comes into the Fusion Center and will be the point of contact between his/her agency and the Fusion Center. Agency representatives will be responsible for receiving and sharing information in the Fusion Center. Because each agency will have a designated representative to the Fusion Center, the VISWIG will no longer be necessary and will be dissolved a year after it opens.

Issue 2 - How can the Commonwealth ensure local participation in the fusion process, both in generating information and in analyzing information and intelligence coming into the Fusion Center?

Recommendations

1. Each locality should have the opportunity to designate a representative to the Fusion Center, who will be responsible for receiving and sharing information.

2. Local Chief Administrative Officers should designate two law-enforcement and two non-law-enforcement representatives to the Fusion Center. The local representatives will be responsible for receiving and sharing information.

3. Localities should be encouraged to share relevant information with both the Fusion Center and the Joint Terrorism Task Force (JTTF).

IV. Working Within the Federal Context

The Federal government is creating an information sharing environment through the National Intelligence Reform Act. The Commonwealth must be prepared and willing to work with the Federal government to establish this environment. This will require working with the Federal government on the handling of Federally-classified and sensitive information, as well as representation at the Federal level.

Issue 1 - How can the Commonwealth best manage the information flow between the Commonwealth and the various Federal entities?

Recommendations

1. The Office of Commonwealth Preparedness should work with the Federal government to establish appropriate mechanisms for obtaining information and data for the fusion process from as many different sources as possible.

2. Within the DHS, the Homeland Security Operations Center (HSOC) is likely to remain the primary source of information for the Fusion Center. Therefore, the Commonwealth should consider maintaining a representative at the HSOC. Regular reporting to DHS/HSOC will affect local funding streams.

3. The National Guard, reporting for the Defense Department, should have full-time representation in the Fusion Center, giving the State a direct link to the military. This person will be trained in accordance with the fusion process requirements.

4. The FBI, on behalf of the Justice Department, should place an analyst in the Fusion Center. This greatly enhances the exchange of mission-critical information.

5. Information sharing mechanisms in the Fusion Center should also incorporate the Centers for Disease Control, which can report on behalf of the Department of Health and Human Services.

V. Implementing Effective Information Sharing

Effective information sharing at all levels of government and with the private sector will require attention at each step in the information cycle, starting with efforts to ensure all appropriate players are contributing to meeting identified information needs, handling the information appropriately, effectively analyzing that information, and disseminating the information to all those who need it. The consumers of this information must then have a mechanism for updating information requirements as needed.

Getting information into the fusion process

Issue 1 - Policies and procedures must be developed to ensure that information flows into the fusion process in an appropriate way and from as many sources as possible at all levels.

Recommendations

1. Descriptions of how information flows into the fusion process should be included in the Standard Operating Procedures for the Fusion Center, to include:

   - **Who** may submit information, with complete contact data
   - Submission Protocol **(How and When)**

- Types of information to be submitted (**What**)
- Consolidation of information at the local level
- Evidentiary chain-of-custody protocol for physical input (e.g. suspicious substances)

2. All personnel in the information chain should be vetted (background checks, even if they will not require clearances) and receive training.

3. State and local officials should work together to facilitate the gathering and sharing of information so that leads and information can be further developed. Once this occurs, information will be generated and investigated at the State and local levels, and not solely at the Federal level.

4. Procedures should be developed to minimize duplication of investigative efforts.

Analyzing information

For the fusion process to be successful, input is required from all agencies, levels of government, and the private sector. Only then will the Fusion Center analysts be able to connect the dots in all areas to evaluate all hazards to the Commonwealth.

Issue 1 - Analysts in the Fusion Center must understand local and regional issues and have local and regional connections.

Recommendations

1. While it may not be feasible to match Fusion Center analysts to geographical areas in the State, the Center should strive for collective expertise in areas with varying types of concerns and conditions (urban and rural, industrial and agricultural, inland and coastal, etc.).

2. Temporary exchange of personnel with Federal and local intelligence centers or short tours of duty in the Fusion Center for local personnel should be considered to expand understanding of varying viewpoints, develop partnerships, encourage cross-pollination, and establish lines of communication.

Issue 2 - The Commonwealth must ensure the knowledge and expertise of the responder community is brought to bear in analyzing information through the fusion process.

Recommendations

1. The expanded analyst cadre at the Fusion Center should include fire service and EMS through representation from the Department of Fire Programs, agriculture, and the Office of Emergency Medical Services of the Health Department.

2. The Center should maintain regular contact with function-specific analysts from other agencies and the private sector (health and medical, agricultural, transportation, fire services, environmental, military, industry and infrastructure, etc.) and bring them into the fusion process when needed.

3. Secure communication mechanisms should be established to facilitate contacts in risk- and threat-specific arenas (ports, large event managers, high hazard industry, etc.). Outreach and education programs should be developed to encourage and ensure these contacts.

Issue 3 - There should be specific qualifications for the Fusion Center's intelligence analysts.

Recommendations

1. Fusion center analysts should collectively have local/regional (preferably Virginia) government and emergency responder background as well as expertise in the field of intelligence analysis.

2. Virginia should develop a training and education program on intelligence and information sharing:

   - Base level of "what to look for" for wide range front-line workers
   - Mid-level training for localities and agencies in "basic analysis"
   - Higher level training for local and State officials in "detailed analysis and trend recognition."

Handling sensitive information

There are potentially many categories of sensitive information that agencies and entities will be providing to the fusion process—including classified information, law enforcement information, information raising privacy issues, health information, and even proprietary information. There must be clear policies and protocols governing the handling and dissemination of this information, with statewide application.

Issue 1 - State agencies need a system and protocols for managing and protecting sensitive information, including classified information and intelligence.

Recommendations

1. Virginia State Police (VSP) is developing a set of guidelines for the Fusion Center; however, *an Executive Order is needed* to extend these guidelines beyond the Center and beyond law enforcement and intelligence information. The Attorney General should be consulted on these guidelines and any Executive Order to ensure full compliance with legal requirements, particularly as they relate to privacy and civil liberties concerns.

2. Virginia Department of Transportation (VDOT) also has a classification process. This could possibly be expanded statewide.

Issue 2 - What requirements should be in place regarding the individuals who participate in the fusion process but do not hold a Federal security clearance?

Recommendation

State agency personnel and members of the private sector are not required to obtain a Federal secret clearance. These individuals will undergo a State Police background investigation that will allow access to the high-security area of the Fusion Center.

Issue 3 - Which entity will be responsible for disseminating classified information to various agencies, etc.?

Recommendation

The Information Classification Unit (ICU) should forward information to State agencies and the private sector on the basis of mission-related authorization and need-to-know. This will enable the State to share information with people who do not hold a Federal security clearance.

Issue 4 - The State should continue to work for Federal security clearances for as many State personnel as possible.

Recommendations

1. The Office of Commonwealth Preparedness will submit a clearance recommendation list of 30 State personnel to the Department of Homeland Security.

2. In addition, because the overall lack of clearances for State employees outside of the Fusion Center is not likely to change, protocols should be developed for properly "scrubbing" information so it can be disseminated outside the intelligence community. These protocols need to be agreed upon between the levels of government and agencies and should be implemented nationwide.

Issue 5 - Aside from legal restrictions, agencies are often reluctant to share information because they fear that another agency may prematurely act on such information without coordinating the action with the provider agency, thus possibly jeopardizing ongoing efforts or initiatives.

Recommendations

1. When the Fusion Center disseminates information, the lead action agency should be noted for reference and as a point of contact for follow-up questions.

2. The National Security Act has clear penalties for improper disclosure of Federal information and intelligence of a classified nature. Once the Commonwealth is capable of implementing its own state-specific

classification system, legislation should be considered to provide penalties for inappropriate release.

Evaluation and Feedback

It is important throughout the fusion process to keep in mind that the ultimate goal is not only information sharing, but also providing decisionmakers at all levels with the information that they need to better understand the threat, vulnerabilities, and ways to manage the risk of a terrorist attack. It is with this objective in mind that consumers of the information—including analysts, first responders, legislators, executive officials, and the Governor—should have a process for providing feedback on the quality of the information and updating information needs. In the world of intelligence, this is often called a “requirements process.”

Issue 1 - How can the Commonwealth best ensure that the fusion process is dynamic, so that it can continually improve and respond to evolving information needs?

Recommendation

A formal requirements process should be established, managed by the Fusion Center, through which all relevant entities would have an opportunity to indicate their information needs and evaluate information provided through the fusion process. Each entity should designate an official who will be responsible for ensuring the entity participates effectively in the requirements process. The Fusion Center should designate an official to manage the process and ensure requirements are passed on to all entities that are in a position to gather information to meet those requirements.

Appendix I-3

Mass Fatalities Management Task Force of the Secure Commonwealth Panel

Recommendations to
The Secure Commonwealth Panel
And
The Office of the Governor –
Commonwealth Preparedness

July 13, 2005

Table of Contents

Members

The Honorable Jane Woods, Chair
Secretary of Health and Human Resources

William C. Armistead
Disaster Preparedness and Response Director
Office of Planning and Development,
Virginia Department of Mental Health, Mental Retardation, & Substance Abuse Services

Michael Berg
Regulatory and Compliance Manager
Virginia Department of Health

Brett Burdick
Director, Technological Hazards Division
Virginia Department of Emergency Management

Michael M. Cline
State Coordinator
Virginia Department of Emergency Management

Colonel Michael Coleman
Deputy Chief of Staff Operations
Virginia National Guard

Marla Decker, J.D.
Deputy Attorney General
Public Safety & Enforcement Divisio**n**
Office of the Attorney General

Paul B. Ferrara, Ph.D.
Director
Department of Forensic Science

Marcella Fierro, M.D.
Chief Medical Examiner
Virginia Department of Health

Lori Hardin
Statewide Mortality Planner
Office of the Chief Medical Examiner
Virginia Department of Health

Gail D. Jaspen
Chief Deputy Director
Virginia Department of Health Professionals

John W. Jones
Executive Director
Virginia Sheriffs' Association

Lisa G. Kaplowitz, M.D.
Deputy Commissioner for Emergency Preparedness and Response
Virginia Department of Health

Bruce Keeney
Executive Director
Association of Independent Funeral Homes of Virginia

Art Lipscomb
Legislative Director
Virginia Professional Fire Fighters Association

Constance McGeorge
Special Assistant to the Governor
Office of Commonwealth Preparedness

Susan Motley
Executive Director
Virginia Funeral Directors Association

Major Robert B. Northern
Deputy Director, Bureau of Field Operations
Virginia State Police

Bud Oakey
Managing Director and CEO
Advantus Strategies LLC

Mandie Patterson
Victim's Services Section
Department of Criminal Justice Services

Dana Schrad
Executive Director
Virginia Association of Chiefs of Police

Tricia Snead
Manager, Disaster Assistance/Emergency Planning
Virginia Department of Social Services

Robert B. Stroube, M.D., M.P.H.
State Health Commissioner
Virginia Department of Health

Richard E. Trodden
Arlington County's Commonwealth's Attorney

Elizabeth Young
Executive Director, Virginia Board of Funeral Homes and Embalmers
Virginia Department of Health Professionals

Introduction

I am pleased to submit to the Secure Commonwealth Panel the report from the Mass Fatality Management Task Force.

The Virginia Secure Commonwealth Panel was tasked overall with assessing the state of the Commonwealth' s preparedness and security in response to the all-hazards terrorist attacks threatening the United States since September 11, 2001. All aspects of the lives and activities of the citizenry have been under review for issues relating to health, safety and security in order to develop recommendations for improving the security of—and the official and societal response to—a mass fatality event and to enhance the survival of the citizens. The latest round of panel task forces has dealt with intelligence and information sharing, funding, public/private cooperation, and performance measures and has developed recommendations for decisionmaking and changes in statutes and public policy.

The Mass Fatality Management Task Force was specifically charged "to go beyond operational issues to address decisionmaking and statutory and public policy issues regarding mass casualty events."

To accomplish this task, public and private parties that interface with the death event met to identify and address issues relating to mass fatalities. A mass fatality event, from an all-hazards point of view, would include fatalities due to naturally-occurring weather events such as floods or earthquakes, and to terrorist events resulting in thousands of deaths, either all at once, as in attacks on the World Trade Center and Pentagon, or over time, as in the case of a biologic attack epidemic such as the Virginia anthrax bioattack.

The panel brought together agency representatives from the Governor's Office of Commonwealth Preparedness, Department of Health, Office of the Chief Medical Examiner, Emergency Management, Emergency Medical Services, Virginia State Police, Health Professions, Criminal Justice Services, Mental Health, Office of the Attorney General and Commonwealth's Attorneys, and Department of Military Affairs. Private sector collaborators included representatives of Funeral Homes and Embalmers, Virginia Professional Firefighters, Virginia Association of Chiefs of Police, and lobbyists for the funeral service sector.

I believe you will find that the background information and recommendations contained herein meet or exceed the task force's charge and provide the Commonwealth with sound suggestions for measures that will enhance our collective and regional preparedness. I extend my thanks to all the task force members who gave generously of their expertise and time; but especially we all owe great thanks to Dr. Lisa Kaplowitz, M.D. and Dr. Marcella Fierro, M.D. for their unflagging dedication and commitment to this work.

Mission of the Task Force

The mission of the Mass Fatalities Management Task Force is to identify decisionmaking, statutory and public policy issues the Commonwealth would face in the event of a mass casualty incident and make recommendations to the Secure Commonwealth Panel and the Governor's Office of Commonwealth Preparedness on how best to address these issues prior to a mass casualty event to better prepare the Commonwealth for an effective and efficient response effort.

Policy Issues

- Determine how to best address outstanding administrative issues the Commonwealth would face following a mass casualty event

- Determine which legal issues the Attorney General's Office should review and how best the Commonwealth might address these issues

- Identify which departments and agencies require funding to train for and respond to a mass casualty event

- Determine what is required to successfully set up and maintain a Family Assistance Center (FAC) after a mass casualty event

- Determine how best to address issues the Commonwealth would face in a mass casualty event that would require legislation to ensure an effective response.

Recommendations

I. Administrative Issues

Crisis Response Teams and Volunteers

A new policy should be developed regarding how best to staff, train, utilize, and protect the Office of the Chief Medical Examiner (OCME) crisis response team and the volunteers (to include first responders, medical examiners, etc.) who respond to a mass fatality event in Virginia.

Issue 1 - A Disaster Mortuary Response Team (DMORT) is a group of essential personnel who respond to mass fatality events. The Federal government supports Federal DMORT teams that States request for assistance. Historically, DMORT teams have been supplied to jurisdictions that had few or no resources for managing an event or have experienced overwhelming casualty events. The September 11 plane crash in Pennsylvania is an example of the former. The World Trade Center, where they continue to recover fragments of victims for identification, is an example of the latter. Virginia's Medical Examiner System, with the addition of some supplemental resources, could have managed the Pennsylvania event as well as the event at the Pentagon. In any series of multiple coordinated terrorist events, Federal DMORT teams may not be available to supplement Virginia capabilities if they are deployed to jurisdictions with fewer resources. Given Virginia's high-risk status, as evidenced by the Pentagon and anthrax attacks, Virginia needs to supplement the core elements of a Virginia OCME DMORT team that are already in place within the Medical Examiner System.

A DMORT team usually consists of a certain number of team management personnel, forensic personnel, disaster scene personnel, morgue personnel, and staff to operate and manage the Family Assistance Center (FAC). However, the Commonwealth is lacking personnel to support various positions on the DMORT team.

The sidebar on the next page contains a list of essential personnel for a DMORT. The first number indicates the "normal" number of positions on a team; the second number indicates the OMCE capabilities to fill the position with current staff. "V" indicates a plan to fill with volunteers. "Inv" indicates an investigator position needing to be filled to accomplish the task.

<u>Recommendation</u>

Establish 12 full-time equivalents and funding for medical investigators to give the Commonwealth more personnel who can provide staff support in a mass casualty event.

Issue 2 - How can the State best utilize volunteers in a crisis event given tasks, confidentiality, evidentiary issues, and liability?

Recommendations

1. Working with the Virginia Funeral Directors Association (VFDA)—which will serve as the lead funeral group), the Association of Independent Funeral Homes of Virginia (IFHV), and the Virginia Morticians Association (VMA) the OCME, will identify funeral service licensees who are willing to be volunteers. The OCME will ask for Emergency Preparedness and Response funding from the Virginia Department of Health (VDH) for criminal background checks.

2. The Virginia State Police (VSP) will complete initial volunteer background checks during training of the volunteers. Additional background checks will be completed, as necessary, for those who are utilized in a crisis event.

3. OCME will obtain the list of people (funeral service licensees and physicians) who are willing to volunteer in a mass casualty event from the Department of Health Professionals in order to proceed with training and initial background checks.

Disaster Mortuary Team (DMORT)

Team Management
- **Chief Medical Examiner (1, 1)**
- **Assistant Chief Medical Examiner (1, 11)**
- **Administrative Officer (1, 1)**

Forensic Personnel
- **Pathologist (3, 11)**
- **Odontologist (3, VA dental team))**
- **Dental Assistant (3, as team provides)**
- **Anthropologist (3, 2)**
- **Fingerprint specialist (3, DFS will supply)**

Disaster Scene Personnel
- **Search/recovery personnel (12,4 OCME) Inv. & V**
- **Cadaver dog handlers (3,0) *will request Fairfax team**
- **Surveyors/gridders (3,0) Inv.**
- **Body recovery (5,0) Inv. & V**
- **Underwater recovery (4,0)**

Morgue Personnel
- **Body tracker (16, 0)**
- **Mortuary Officer (6,4) Inv.**
- **X-ray technician (3, 0)**
- **Photographer/videographer (12, 0)**
- **Medical records technician (6,6)**
- **Supply officer (4,0)**

Family Assistance Center
- **Mortuary officer 10, 0**
- **FAC manager**
- **Interpreters (3, 0)**
- **Support Personnel**
  - **Mental Health/CISD Specialist (1,0)**
  - **Communications manager (3,1)**
  - **Safety Officer (1, 0)**
  - **Equipment operator (1,0)**
  - **Team Physician/PA/Nurse (1,0)**
  - **Security officer (3,0)**

Issue 3 - The Medical Examiner must ensure the safety of those handling contaminated remains and the safety of the public.

Recommendations

1. Consider amending the Code of Virginia to provide the Health Commissioner with the authority to make the judgment call on the

safety of the return of human remains after a chemical or biological attack. This decision should be made in conjunction with political and health officials.

2. Explore a Bio-Watch program—which is an early warning system—to detect biological agents through continuous air sampling throughout OCME Morgues and multiple indoor detection sensors in the coolers and over the autopsy tables.

3. To protect the staff of Funeral Directors, the VDH should work to implement precautions developed by the National Funeral Directors Association.

Issue 4 - How many staff can/will actually report to a mass casualty event?

Recommendation

OCME will periodically survey its staff for availability to volunteer in a crisis event and will add ability to respond to position descriptions.

Issue 5 - Following a mass casualty event the OCME and the lead law enforcement agency should be called in to evaluate the situation and make determinations on the appropriate specialized skills needed. Historically, through drills and exercises, other agencies that are not subject matter experts (forensic scientists) have called DMORT without first consulting OCME. Despite many of the same "lessons learned" statements following drills, OCME continues to be left out of drills and exercises and anticipates the same will occur again.

Recommendation

The OCME and the Virginia Department of Emergency Management (VDEM) are the organizations that will need to identify the personnel that medical examiners will need for body management so that the Governor can request these personnel in accordance with standard procedures.

Issue 6 - The OCME has not been eligible for grant funds (as it is a statewide rather than local organization) to train the funeral service licensees and other forensic specialists in mass fatality event response.

Recommendation

It is anticipated that VDH will take a lead role in providing training to potential volunteers in advance of actual need; however, OCME requires funds to train its volunteer specialists.

Jurisdiction

It is vital that the various levels of government and agencies that will respond to a mass casualty event understand who has jurisdiction and/or will take the lead during the response and recovery efforts following the event.

Issue 1 - Jurisdictional issues on the management of the deceased are too vague and unclear in the National Response Plan.

Recommendation

The Virginia Department of Emergency Management (VDEM) and the Office of the Attorney General (OAG) will try to develop a Memorandum of Understanding (MOU) with Federal authorities that clarifies jurisdiction in a mass casualty event in the Commonwealth. VDEM will take the lead to initiate these discussions by 9/1/05. Discussions will include OCME, VSP and VDH from the State. The Department of Homeland Security will determine which Federal entities should attend.

Issue 2 - Public Safety and Health entities must recognize and consider “conflicts” prior to an event of this magnitude in order to prevent the rise of jurisdictional issues during and after a crisis event. This will enable these entities to work together to plan for and respond to a crisis more efficiently and effectively.

Recommendation

Policy planners for Public Safety, VDH and OCME should develop MOUs and meet once a year to refine these agreements. The Federal Bureau of Investigation (FBI); VSP and local law enforcement; Medical Examiners; the Virginia Department of Social Services; and the Department of Mental Health, Mental Retardation and Substance Abuse Services (DMHMRSAS) should all be included in these agreements. The OCME and the State Health Commissioner will initiate contacting someone at the Federal level to expedite implementation of this recommendation.

Issue 3 - The OCME should be the only agency (in conjunction with the local community leadership) that is authorized to approve the establishment of morgues in mass fatality events under the jurisdiction of the OCME. In both the 9-11 Event at the

World Trade Center and the Determined Promise 2004 (DP04) exercise in Virginia, non-medical examiner organizations identified and opened morgues without the knowledge of the OCME. In New York, so many agencies opened morgues without the OCME's and Police Department's knowledge that it was unmanageable. Some unauthorized morgues had policies to strip all remains and store the physical evidence in lock boxes, which severely hampered victims' identification (physical evidence should only be removed in the morgue after documentation). Other morgues were allowing any person to enter and view the remains, even if the persons were not next-of-kin. In DP04, the Central Regional Department of Health selected the two largest food distribution warehouses in central Virginia as morgues, which would have resulted in the Commonwealth purchasing and compensating two retail corporations for their losses.

Recommendation

The OCME should be the final approval authority for any morgue, and for its management (if the OCME is the jurisdictional authority for the event). This will better enable the State to coordinate and manage the storage and handling of physical evidence as well as human remains. Access to morgues is an OCME procedure

Communication

The various State health agencies need a reliable communication system to enable them to coordinate the response and recovery efforts after a crisis event.

Issue 1 - Include the OCME in any communication plans to be developed by the VDH. Currently, 45% of deaths in Virginia occur in hospitals. A better communication system will enable hospitals to interface with OCME to report any suspicious deaths in a timely manner.

Recommendations

1. VDH should include the OCME in any communication plan that connects the VDH with hospitals.

2. Programmable radios should be available to the OCME in a multiple fatality event. Brett Burdick at VDEM will be the lead on this project to determine how many radios are required and what functions they should include.

3. VDH will work with OCME to coordinate a better communication system with regional hospitals.

Issue 2 - The need to reform the National Incident Management System (NIMS) to include medical examiners and coroners in the communication/decision process. The

NIMS/Incident Command System (ICS) does not properly address the functional tasks of the medical examiner in the response protocols. The ICS stops at the point where patients die in triage and a "Morgue Manager" is assigned to protect the remains. ICS does not address the incorporation of the medical examiner into the system; therefore first responders think once the Morgue Manager is established the issues go away.

Recommendations

1. Include the OCME in the unified command with the operational law enforcement investigative agencies to develop appropriate incident action plans.

2. Other agencies may also have to be included in the unified command structure—for example, those managing the Family Assistance Center, those mitigating the contaminates on the remains, etc.

3. Fire Programs will lead training and incorporate new plans into this system.

Issue 3 - The National Response Plan does not address mortuary affairs appropriately. There is no reference to law enforcement's role in death investigations, forensic examinations, family assistance, personal effects management, criminal investigations, death notifications to families, and release and dispositional matters.

Recommendation

Virginia VDH personnel are on working groups interfacing with the Department of Homeland Security (DHS) and the National Incident Management System Integration Center to provide feedback on the newly-developed plans for the Federal response. This task force recommends that these groups include the OCME's State Medical Examiner to provide input into these plans and be part of the working groups for the DHS/State revisions to the National Response Plan.

Fatality Management

It is essential to determine how best to identify, transport, and dispose of human remains in a mass fatality event, as well as how to protect the personnel handling the remains.

Issue 1 - The State needs to determine if the identification process in highly fragmented cases will include the testing of ALL tissue, or if only an amount of tissue sufficient to identify all the victims will be processed (the remainder will be considered "common tissue"). Does the State identify all of the victims or all of the pieces of human remains?

Recommendation

If the event is a closed event, meaning all of the victims are known and subsequently identified, identification of human remains will cease and a respectful final disposition made of the "common tissue". If the event is open, meaning all of the victims are not known, the State will work to identify all of the "common tissue."

Issue 2 - Will the State have access to Dover? Virginia was denied access in the Determined Promise 2004 drill despite legislation specifying that Virginia is allowed access to the Dover Air Force Base Port Mortuary in a mass fatality event.[2]

Recommendation

Negotiations are currently underway between the Commonwealth and the Federal Secretary of Health and Human Services to ensure the State will have access to this mortuary should a mass fatality event occur.

Issue 3 - The State needs a policy on how to transport contaminated remains within the State and across state and/or international borders.

Recommendation

Under the funeral licensee laws, transportation services are available from licensed funeral service establishments and from registered surface transportation removal services. The State should determine if there is a Federal regulation for transportation of human remains and if an MOU if possible. Otherwise the State should proceed to move remains as needed.

A(vi)[2] Joint Publication 4-06, in both the 1996 version and the current version (under revision) state: "The use of the Dover Air Force Base Port Mortuary is an option available to civilian authorities." There are no caveats in the publication on distance of authority, state, city, county authorities, etc.

Reporting - Format and Structure

Following a mass fatality event, it is essential that the response teams are able to adequately document action taken. Reporting is a vital tool that, if streamlined and structured, will better enable decisionmakers to determine what next steps need to be taken for the safety of the Commonwealth as well as to limit confusion during and after event response.

Issue 1 - There are no common forms or format for Emergency Operations Center needs requests. Each request is reformatted and reinterpreted. There should be national standards to address this issue. In drills where the OCME has been able to submit requests for additional services, the requests were rewritten and misinterpreted by Emergency Support Functions (ESF 8) staff in the Virginia Department of Health Emergency Coordination Center (ECC)/State Emergency Operation Center (EOC) or in the local EOC. If the OCME were permitted to submit its own requests for the required services, and if each agency utilized the same form while cross-referencing the tracking numbers on the form, the original intent of the request would be maintained and the required resources would be obtained.

Recommendations

1. A uniform request form/format should be developed that can be utilized by local, State, and Federal agencies.

2. Web EOC (Emergency Operation Center) is a system under development that will create a single form for everyone to use. VDH and VDEM are leading this initiative. It should be completed by the end of the year.

Issue 2 - The State has a fragmented reporting structure with no real-time direct contemporaneous reporting 24/7. Reports on medical examiner cases other than homicides, suicides and deaths suspicious for violence are often delayed. The waiting period for receipt of reports from local medical examiners at district offices can be measured in days to weeks to months. These delays inhibit the capture of deaths due to infection that could appear to be natural but might actually be caused by bioterrorism or emerging infections.

Recommendations

1. The OCME needs all deaths reported directly in real time 24/7 by local medical examiners and investigators to a district office, where in-house trained medical investigators can advise on jurisdiction, screen for bioterrorism and emerging infections, and make the real-time determination of management. (This could serve both local medical examiners and localities lacking a local medical examiner. It should also capture bioterrorism deaths masquerading as natural deaths out of hospitals.)

2. Virginia should provide 12 full-time equivalents for medical investigators and funding to enable 24/7 direct submission to district offices of all death reports contemporaneously. The usual reporters are medical examiners, law enforcement, hospitals, and EMS. These additional staff and funds would allow for screening for bioterrorism and infectious death and reporting in real time for determination of jurisdiction and management.

3. To assist first responders with reporting, pocket cards with Med-X signs/symptoms and OCME contact information were distributed. (This will alert first responders when a report should be made to the local medical examiner and provides them with the necessary contact information so the report can be made in a timely manner.) *OCME is working to develop a CD of these pocket cards to give to organizations that can then disseminate the information. This effort to educate more first responders across the state is an inexpensive and efficient approach.

Public Relations

A key aspect of dealing with a mass fatality event is successfully communicating with the public in terms of what citizens can expect from government and medical officials and how family members can best assist the response teams in identifying lost loved ones.

Issue 1 - The State will need a committed VDH public relations person to coordinate dealing with the media/families on fatality management issues.

<u>Recommendation</u>

VDH has secured Jeffrey Caldwell as the official Public Information Officer (PIO) for the OCME. He will receive training in the current public relations crisis plan along with the four regional PIOs and any other PIOs who have not yet received training in this area.

Issue 2 - The Commonwealth needs to develop policy standards that are acceptable to the public with regard to expectations of identification of human remains.

Recommendation

Virginia must develop standards within *each* event as to what is reasonable to do with regard to identifying human remains. Once these standards are developed, the State will need to train the Public Information Officer on these standards so no promises are inadvertently made to the public that the health professionals and government cannot keep.

Issue 3 - The Commonwealth needs to establish a Family Assistance Center (FAC) plan with strict policies covering which agencies may accept reports on missing persons, what information is collected, who interviews the families on personal characteristics of missing/deceased victims of disasters, and who may receive the information. This will prevent confusion among the families and officials as well as prevent agencies from duplicating efforts and inadvertently providing conflicting information.

Recommendations

1. The FAC should be the only authorized site to collect information on missing persons via interview or password accessible website.

2. Identification and access to information will be limited to next-of-kin or a designated person assigned the password. The next-of-kin or designee should be fingerprinted for security and fraud prevention.

3. The DMORT Victim Identification Form will be used for information collection and to promote interoperability.

Issue 4 - The Commonwealth must continually educate the public and crisis event response teams on how to best deal with/respond to a mass fatality event.

Recommendations

1. Include OCME in meetings, drills, and working groups throughout the Commonwealth to allow fatality management and first responders to plan for and practice this portion of the exercises.

2. Connect with local EMS councils to begin the process of educating first responders on alerting local medical examiners about a drill or actual incident.

3. Inform OCME of the statewide exercise calendar and invite them to attend these drills.

4. Public Information Officers should be trained in educating the public, as well as state agencies, on how to best deal with a mass casualty event.

II. Attorney General Issues

Fraud Mitigation

Mass fatality incidents have historically resulted in cases of fraud by some members of the public. Lessons learned from the World Trade Center attack on 9/11 indicate fraud has been a major problem. Two examples of fraud that has occurred in past events are: persons assume new identities and their families report them dead or missing to receive entitlements; next-of-kin, survivors, and others have reported that "high valued" personal effects on their loved ones are missing and have attempted to sue the state for the "return" of the items.

Issue 1 - How can the Commonwealth best reduce the risk of fraud following a mass fatality event?

Recommendations

1. The Family Assistance Center (FAC)/OCME should develop an online system of reporting. OCME will work with the Department of Social Services to develop this system.

2. The agency with the authority to receive reports should have legal authority to require families and individuals who are reporting missing persons to make sworn affidavits on the reports to allow for "false reports" follow-up.

3. A policy should be established designating the FAC as the only agency responsible for receiving missing persons reports.

4. Reporters of missing persons, beneficiaries of entitlements, and those trying to claim personal effects should be required to provide identification and submit to fingerprinting for identification checks. *Everyone must ultimately report to the FAC for verification of status as next-of-kin.

5. To preserve personal effects and evidence, access to remains should be strictly limited to authorized persons who have crime scene and forensic documentation training to ensure personal effects are properly documented and recovered at scenes. *Hospitals also should be made aware of proper documentation of physical evidence for patients.

6. The OCME will liaise with the Cemetery Board to enable better coordination with them in the event of a crisis.

Issue 2 - The Commonwealth must be able to determine a clear and identifiable next-of-kin or legal guardian to ensure the release of information to the proper people.

Recommendations

1. The Office of the Attorney General will provide and promulgate a legal definition of “next-of-kin”.

2. Legislation may be necessary to identify who is legally in line to receive remains and personal effects of victims after a mass fatality event.

Property Disputes

Personal effects management will involve returning the effects to the legal next-of-kin. The likelihood of property disputes is high, and the Commonwealth should determine how best to address these dilemmas.

Issue 1 - The Commonwealth should develop a protocol for property disputes over personal effects from a mass fatality event.

Recommendation

Policies should be established for the identification of legal next-of-kin and the procedures to follow if disputes arise.

Volunteers and Crisis Response Teams

The Commonwealth will need to address the various legal issues regarding liability protection for volunteers.

Issue 1 - Dentists, anthropologists, funeral service licensees etc. who respond and operate under the supervision of the OCME require a definition of status that will cover their person in the event of injury while responding to the OCME’s request for assistance.

Recommendation

Determine whether volunteer workmen's compensation already exists and cite the Code section stating the same.

Issue 2 - Are OCME volunteer responders covered under the Volunteer Medical Liability Act passed by the General Assembly in 2005?

Recommendation

Clarify this issue in writing.

Human Remains

The Commonwealth needs to develop policies and procedures for the identification and disposition of human remains.

Issue 1 - Following a mass fatality event, various agencies will be required to collect and coordinate information to mitigate the situation. To accomplish this task, information that is not normally shared or authorized for release will have to be shared. The presumption has always been that the OCME may request information from healthcare providers to assist with identification of deceased persons.

Recommendation

The Office of the Attorney General will clarify what information the OCME is legally permitted to request and obtain to identify physical remains from surviving as well as deceased patients, as limbs may be found that belong to people who survived the event.

Issue 2 - Bodies that are hazardous may need to be transported intra- and interstate for examination. What authorization is needed, if any?

Recommendation

The Office of the Attorney General will review the Code of Virginia to determine the conditions—if any—under which funeral service licensees or transporters may drive contaminated or highly suspicious remains over the roadways without Department of Transportation permits and placards.

Issue 3 - Mass fatality events will result in unidentified body parts and some identified persons who will not be claimed. The Virginia Department of Environmental Quality, VDH, OCME and other responsible agencies should pre-identify possible locations where hazardous, unidentifiable or unclaimed remains may be interred.

Recommendations

1. The Department of Environmental Quality, VDH, OCME, and other responsible agencies should pre-identify possible locations where hazardous, unidentifiable, and unclaimed remains can be interred.

2. The Code of Virginia should address how cemetery owners will be protected if the remains are safe for burial, yet considered to be "hazardous".

III. Budget Issues

Personnel Costs

The Commonwealth must ensure there are enough personnel to respond to a mass casualty event, and that the personnel have up-to-date training in disaster response.

Issue 1 - What personnel expenses will the Commonwealth incur on a one-time and recurring basis?

Recommendations

1. The Commonwealth's number of medical examiners is dropping steadily, with fee identified as a major issue. Local medical examiners are down from 430 in 1994 to 283 in 2004 and 250 at present. The Board of Health considered medical examiner expertise, time and fees and recommended and authorized a fee increase to $150 per case. Requests for a fee increase from the General Fund failed to survive in 2005 in the Governor's, House or Senate budgets. The State should re-consider General Fund funding of a fee increase. If this is not possible funds should be requested from homeland security funds or from Tobacco Settlement money. The cost is $616,000 in the first year with a recurring cost and estimated yearly increase of $30,000 for a projected increase of 200 cases per year at $150/case.

2. The Office of the Chief Medical Examiner needs 12 more investigators for direct reporting, 24/7 MED-X bioterrorism surveillance, and investigation. The system now has eight investigators to cover two shifts on weekdays. The system fills in with part-time, fee-for-service, day-by-day investigators. The learning curve is steep for intake screening and scene management, and there is no follow-up by part-time investigators on case

questions. Salary plus benefits for 12 new investigators: $70,000 x 12 = $840,000 (recurring). 24/7 investigator coverage to receive information (see above) and a secure dedicated server: $15,000.

3. The OCME has 149 independent jurisdictions, 35 health districts, six hospital regions, three Metropolitan Medical Response Systems, and over 100 military commands to interface with. The one current statewide planner is not physically capable of interfacing with all the organizations and required drills despite numerous hours of overtime and traveling throughout the State. Thus the State should hire one additional Emergency Planner for OCME districts' training and planning, to be stationed in the highest risk area of Northern Virginia to work with Capitol Region Planners. Salary Plus Benefits $60,000 x 1 = $60,000 (recurring).

Preparation and Training Costs

Training and staffing will be required to properly operate the Family Assistance Center (FAC). To ensure efficient and effective management of this vital part of a mass casualty event response, the Commonwealth must budget for recurring and one-time costs of readiness for the Department of Social Services (VDSS) and the Department of Mental Health, Mental Retardation and Substance Abuse Services (DMHMRSAS).

Not only does the FAC provide a means for securing essential information, it also provides either direct or referral services for the living family members who are seeking grief and mental health counseling, guidance on funeral preparations, and information about insurance questions, financial assistance programs and social security issues, etc. It is therefore important that Commonwealth agencies authorized as lead for the FAC have adequate staff and training to serve the needs of the living.

Issue 1 - The Virginia Department of Social Services (VDSS) needs one Planner and one Trainer to meet its responsibilities in planning, exercising, developing procedures, and training staff. With the Department of Social Services serving as the lead agency for the FAC and DMHMRSAS serving as the lead partner, the addition of two staff, dedicated to emergency services, for each agency will improve our response and recovery efforts by insuring dedication of required time for planning and training for various responsibilities during mass casualty events.

Recommendations

1. VDSS will need the funds to properly train the people who are to staff and run the FAC in the event of a crisis. DSS cost of training and travel ($400 x 50 staff) =$20,000. One time cost of office set-up for two new staff = $8,000. Salary plus benefits and travel $65,000 x 2 = $130,000 (recurring).

2. DMHMRSAS cost of training, travel, and revenue replacement loss due to staff being sent to FAC training, $1500 x 110 (two per community service board and two per facility) = $165,000. One-time cost of office set-up for two new staff = $8,000. Salary plus benefits and travel $150,000 x two = $300,000 (recurring).

3. The Commonwealth should budget $50,000 for recurring volunteer and local medical examiner training sessions.

4. The Commonwealth should budget for volunteer and local medical examiner background investigations, at $50/investigation x 350 = $17,500.

Travel and Equipment Costs

The Commonwealth will need to fund travel and equipment expenses to prepare for and respond to disasters.

Issue 1 - What travel expenses will the Commonwealth incur on a one-time and recurring basis?

Recommendations

1. The OCME will need vehicles for body transport and staff transport to use daily and during disasters. OCME is unable to use pool cars for day-to-day and transport (biohazard) usage, and will thus need two cars/vans at $20,000 x 2 = $ 40,000 (One time, five year.)

2. The Command Center/Medical Examiner Response vehicle will need to be shared with the VDH and Vital Records. The VSP has been in the market for a used vehicle for OCME for some time. The state would incur a $300,000 (one-time) cost and a $3,000 yearly maintenance cost for this vehicle.

3. The Commonwealth should budget $10,000 a year in operations travel for meetings with mutual aid States and for statewide training.

Issue 2 - What equipment expenses will the Commonwealth incur on a one-time and recurring basis?

Recommendations

1. The Medical Examiner must ensure the safety of those handling contaminated remains and the safety of the public (Biowatch Program). OCME will give VDEM a list of supplies needed during a mass fatality event. Cost of keeping a rotating store of supplies to get through three days of an event until other supplies arrive: $75,000 (one time).

2. Outside storage space must be accessible to the OCME. Current buildings are at maximum capacity already with normal supplies. Rental costs: $1000/month (recurring).

3. Web-based communication equipment is needed for interfacing with FAC, hospitals, and EOC centers. The State should budget for a $100,000 (one-time) purchase of Web-EOC and other computer based information sharing equipment.

4. OCME has no internal State resources for DNA identification services. Following the last plane crash, families paid for the DNA testing on the victims to get the remains released. Estimated annual cost for normal DNA ID is $10,000 at $500/test. For a disaster the cost could reach in the millions. NYC as of April 2005 has spent $100 million on identification alone. The Commonwealth will need an MOU with the FBI or others to perform testing.

IV. Family Assistance Center (FAC) Issues

Coordination and Staffing

OCME staffing does not allow for the administration and management of a FAC. A lead agency needs to be identified with the appropriate legislative authority and funding to support such a function.

Issue 1 - The Commonwealth must designate a lead agency (authority) to form and coordinate the Family Assistance Center after a mass fatality event.

Recommendations

1. The Virginia Department of Social Services (VDSS) should be the designated lead agency in cooperation with the OCME for mortality matters.

2. In addition the Department of Mental Health, Mental Retardation and Substance Abuse Services should be designated as the secondary lead, and all agencies within the Health and Human Services Secretariat should be designated as responding agencies upon request.

3. If the language in the document designating the lead agency clearly states that other agencies within the Secretariat will respond upon request, then it may be more appropriate for the lead agency to simply enter into MOUs with all agencies within the Secretariat.

4. Funeral Service Licensees would be a good training resource for the FAC because they deal with families in these situations on a daily basis.

Issue 2 - The Commonwealth should identify agencies that will provide staffing for a Family Assistance Center.

Recommendations

1. Participants will include State, local, and Federal agencies, as well as volunteer and private organizations. At the statewide level, all the players must be included in the planning process, and MOUs must be established with partners in the private sector and at the Federal level.

2. Key agencies involved should meet to develop procedures.

3. Social Services and designated others must to be trained in completing the Disaster Mortuary Team Victim Identification Form that will be used to collect information at the FAC.

Preparation

If the FAC is to be a successful operation it is imperative that the needs of the living be compassionately addressed and that the necessary public/private resources are appropriately trained and tools available.

Issue 1 - What training will FAC personnel need to provide the best assistance to families affected by the disaster?

Recommendation

An organized and well-managed Family Assistance Center is the direct interface between the local governments and the Commonwealth of Virginia following any disaster. For the OCME it is essential to get the information from the families necessary to identify the victims. Even if there are no deaths, the government must have a mechanism to efficiently provide services to the public. Grants or other funds should be found to provide all of the participating agencies with the resources to develop and exercise FAC plans in Virginia.

Issue 2 - A data system is required to support a FAC for several purposes:

- To collect information on families and persons reporting their loved ones missing. The system should also allow for Web based reporting for those who cannot travel to the FAC.
- To track case histories on families and the services they received, are entitled to, and what has been for done or said to them before. This is to prevent victims from having to repeat their story to each agency they encounter and to enable caseworkers to understand each family's case history. NTSB has a program such as this.
- To provide families and the public with information on the incident and the services available (such as the 211 system established) and detailed descriptions of the procedures each agency is performing (e.g., what is DNA and how is it collected and used in the identification process); and to transmit the transcripts of the family briefings given each day (MCI can do this as part of a contract with telephone bridges for those families who cannot travel to the FAC.)

Recommendation

The OCME needs to implement a tracking system that is interoperable with the Disaster Mortuary Team and National Transportation Safety Board in order to make Virginia forms as interoperable as possible.

Issue 3 - What equipment is needed for a FAC? Who will fund, store, and set equipment up?

Recommendations

1. Establish a photographic identification card with bar code tracking systems for processing for families and FAC workers. This will enable the FAC to check in families to their stations. Each employee interfacing with the families can be tracked in the case histories, and the locations of families in the FAC can be easily traced in case they are required to report somewhere for information or services.
2. Identify what VDH can do to connect OCME to hospitals to interface with their patient tracking systems.
3. A variety of office equipment will be needed (telephones, fax machines, etc.). Establish and fund the facility/space requirements for a FAC.
4. Determine if DHS will cover costs of an FAC operation if a Federal declaration is received. FAC is not addressed in the National Response Plan.

V. Legislative Issues

Crisis Response Personnel

Currently only the full time staff of the OCME is identified as first responders in the smallpox immunization plan for VDH EP&R. Will this policy apply to all other first responder programs in the Commonwealth?

As defined in the December 17, 2003 *Homeland Security PresidentialDirective/HSPD-8*: " d) The term 'first responder' refers to those individuals who in the early stages of an incident are responsible for the protection and preservation of life, property, evidence, and the environment, including emergency response providers *as defined in section 2 of the Homeland Security Act of 2002 (6 U.S.C. 101*), as well as emergency management, public health, clinical care, public works, and other skilled support personnel (such as equipment operators) that provide immediate support services during prevention, response, and recovery operations."

Issue 1 - OCME and all supporting staff (Funeral Service Licensees, Dentists, Anthropologists, etc.) must be legally identified as first responders in Virginia.

Recommendation

A provision should be made to allow for voluntary immunization when indicated and for prophylaxis as needed when managing medical examiner cases at the medical examiners' request. Cost is to be determined.

Disposition of Human Remains

The State must determine how best to dispose of human remains and memorialize the burial so it will be more acceptable to the public.

Issue 1 - Following nearly every mass fatality incident, the government has erected a memorial for the deceased. Traditionally, those unidentified remains or "common tissues" which cannot yield a positive identification have received respectful final disposition in a manner acceptable to the surviving family members.

Recommendation

Pre-planning for this activity should be considered with a lead agency identified and policies developed on who shall serve on a board with the family representatives to determine what final disposition is best for the particular incident.

Issue 2 - The State Model Emergency Health Powers Act of December 21, 2001 provided good guidance for health departments and legislative bodies on addressing human remains disposition. This guidance was not included in any of the emergency declarations developed in the last three annual legislative assemblies for the Commonwealth of Virginia.

Recommendation

Insert policy guidance into Virginia's Emergency Declarations.

Conclusion

Task force members identified insufficient Medical Examiner staff and budget to develop and support mass fatality management efforts in Virginia. The task force categorized its recommendations for improvement into four groups – administrative, Attorney General issues, budget issues, family assistance center issues and legislative issues.

The major administrative issue was insufficient staff in the Medical Examiner System and a fragmented death reporting system to support core activities for surveillance and crisis response. The task force recommends that 12 full-time examiner positions be established and funded to enable direct contemporaneous reporting of the 50 percent of Virginia deaths that occur out-of-hospital. The examiners would also be the on-scene medical management team for body recovery and evidence preservation. These positions would be part of the core of Virginia's own disaster mortuary operations team, a Virginia "DMORT." The task force also recommends implementation of screening by MED-X, the Center for Disease Control bioterrorism surveillance program for out-of-hospital deaths.

A second major issue identified was the extent to which personal identification efforts would be carried out. The task force recommends that for closed events identification efforts would cease when all are identified, whereas for open events all recovered remains would be subject to scientific methods of identification.

The Attorney General issues addressed by the Task force involved clarifying Virginia Medical Examiner jurisdiction in relation to that of Federal authorities, fraud mitigation, and property disputes. The task force recommends working with Federal authorities to develop cooperative arrangements and asking the Office of the Attorney General to develop protocols to protect citizen survivors from fraud and safeguard personal property.

The major budget issue is the cost of recruiting and retaining Virginia Medical Examiners who are the front line city and county physicians who identify cases that are suspicious for bioterrorism (anthrax) and emerging infections (SARS, avian flu pandemic) and manage the grass roots death investigation system in Virginia. The number of Medical Examiners has declined from 430 in 1994 to 250 in 2004. The primary reason for resignation is the low case fee. The $50/case fee has not been increased since 1980, while Medical Examiners have been tasked with additional duties of surveillance, evidence collection and increased paperwork. The Board of Health approved an increase to $150 per case, which would require the General Assembly to allocate an additional $840,000 to the Medical Examiner System budget. The request was not included in any of the 2005 General Assembly budget documents.

Virginia has no family assistance center (FAS). The Virginia Department of Social Services has been tasked with establishing a center where families may report missing family members, provide identification information and receive the other supportive services needed in times of crisis. The Virginia Department of Social Services needs staff and budgetary support for core staff to develop the FAS.

Two legislative issues resulted in recommendations to amend the Code of Virginia. The first would establish medical examiners and supporting staff as “first responders,” which would facilitate prophylactic immunization for bioevent mortality management workers. The second recommendation requests that the Virginia State Model Emergency Health Powers Act of 2001 be amended to provide guidance on the final dignified disposition of unidentified “common tissues” and to make provisions for memorials in honor of mass fatality victims of terrorism.

Appendix I-4

Performance Measures Task Force of the Secure Commonwealth Panel

Recommendations to
The Secure Commonwealth Panel
And
The Office of the Governor –
Commonwealth Preparedness

May 10, 2005

Table of Contents

Preface

The Secure Commonwealth Panel created this task force and charged its members with developing measures to gauge the performance of the Commonwealth and its localities in meeting the challenge of ensuring our overall preparedness in the area of homeland security. This report is our effort to meet this charge, and reflects the views of the task force members. In preparing this paper, we have drawn on the inputs of numerous experts in the Commonwealth, including government officials and individuals in the private sector and academia. We thank them for their important inputs. At the same time, however, we acknowledge that the responsibility for the contents of this report are our responsibility only, and not that of the organizations with which we are associated.

Thanks also go to Megan Stifel of Sutherland Asbill & Brennan and Mary Warder of the Office of Commonwealth Preparedness for their significant contributions and assistance in the preparation of this report.

Jeffrey P. Bialos
Task Force Chair &
Rapporteur

Members

Jeffrey P. Bialos, Chair
Partner, Corporate
Sutherland Asbill & Brennan LLP

Janet L. Clements
Deputy State Coordinator
Department of Emergency Management

BG (Ret.) Manuel R. Flores
State Director
Selective Service System

Dr. Lisa G. Kaplowitz
Deputy Commissioner for Emergency
Preparedness and Response,
Virginia Department of Health

Mike McAllister
Department of Transportation

Jan Sigler
Special Assistant to the Governor
Office of Commonwealth Preparedness

Staff
Megan Stifel
Sutherland Asbill & Brennan LLP

Dr. Vinton G. Cerf
Senior VP, Technology Strategy
MCI

Julian Gilman
Department of Emergency Management

Robert Mathieson
Chief Deputy Director
Department of Criminal Justice Services

Yacov Y. Haimes
Professor, University of Virginia

Suzanne E. Spaulding
Managing Director, The Harbour Group
LLC

John S. Quilty
Retired, Senior Vice President and Director
MITRE Corporation

Capabilities and Performance Measures for Commonwealth Preparedness

One critical element of maintaining a "safe, secure and prepared Virginia" is to establish a set of performance measures to assess how the Commonwealth is performing in meeting its goal of "developing and overseeing a coordinated prevention, preparedness, response and recovery strategy for natural and man-made disasters and emergencies."[3] Performance measures can help in determining the effectiveness of the Commonwealth's preparedness capabilities, in improving their efficiency, and in allocating resources in support of the Commonwealth's goals. [4]

1. "Core" Preparedness Capabilities for Virginia

Establishing performance measures requires establishing a base line set of core competencies or capabilities Virginia must develop in the short, medium, and long term to meet these preparedness goals (i.e., of maintaining an integrated homeland security and emergency capability). These capabilities must encompass all elements of the Commonwealth and its citizenry, including government, the private sector, and the public, and must take into account the relationship of the Commonwealth's activities to those of the Federal government and other state governments.

In the years since September 11, the Commonwealth's focus has been primarily on taking short and medium term measures needed to close clearly identified "capability" gaps rather than on establishing a long-term vision of Virginia's security and ensuring we have the right capabilities to meet those overall needs. Indeed, most of the Federal homeland security grant assistance received by the Commonwealth has been utilized for specific equipment gaps that were identified rather than for training and the development of overall capabilities or protocols. With the passage of time and the completion of many short term tasks, it is now time to plan for the longer term and put in place a full scale, integrated homeland security strategy, including the building of an integrated set of capabilities to prevent and respond to homeland security threats and a system of standards to measure whether Virginia is meeting its preparedness needs.

A(vii)[3] Consistent with these objectives, this memorandum addresses an "all hazards" approach (i.e., it encompasses performance measures designed to address the effectiveness of the Commonwealth's capabilities with respect to both homeland security threats as well as other disasters (man-made and natural). Thus, unless otherwise stated, the discussion herein, and the use of the term "preparedness", relates to "all hazards"; the term "homeland security" capabilities or threats relates solely to such security threats and not to "all hazards."

A(viii)[4] There is a well established literature on performance measures, which highlights that they serve both external and internal agency purposes – in particular in assisting agencies to effectively and efficiently manage their operations and as part of strategic and operational management. See, e.g., Guide to Performance Measure Management, Texas State Auditor's Office, 7-8 (1999).

This report thus sets forth:

1) The core competencies we believe are needed in Virginia as part of an overall "enterprise" approach to developing and implementing a coordinated preparedness strategy for the Commonwealth.

2) Performance standards to measure the Commonwealth's performance in meeting the core competencies identified as intrinsic to preventing, preparing for, responding to and recovering from natural and man-made disasters and emergencies, including terrorist attacks.[5]

2. Key Considerations in Shaping and Measuring Preparedness Capabilities

In developing an enterprise vision of "core" capabilities and related performance measures for Virginia's preparedness, we believe that a number of factors are critical:

A. The Commonwealth homeland security "enterprise" is only one aspect of the overall holistic U.S., and ultimately, global approach to providing homeland security to the citizens of the Commonwealth and other U.S. and foreign jurisdictions. It is important to recognize the limitations of Virginia's role while ensuring that its efforts are fully integrated with, and draw maximum benefits from, those of other jurisdictions. Performance measures adopted for the Commonwealth must recognize the Commonwealth's specific role – and possible limitations – in performing these functions. Performance measures must also gauge the extent to which the Commonwealth and its localities have developed seamless intergovernmental relations that maximize Virginia's preparedness.

B. The Commonwealth homeland security "enterprise" must be consistent with Federal government directives and guidelines, utilize appropriate tools provided by the Federal government, and recognize and adapt to Federal policies on the provision of homeland security grant assistance to states and localities. The enterprise "capabilities" must be developed within the framework of U.S. Homeland Security Presidential Directive-8 on National Preparedness ("HSPD-8") and other pertinent Federal laws, regulations and policies. In particular, the Commonwealth must recognize the following:

- Establishment of the National Preparedness Goal. Pursuant to HSPD-8, the U.S. Department of Homeland Security ("DHS") is developing an overall "national preparedness goal" and defines "preparedness" as the "existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from" domestic terrorist attacks, major disasters, and other emergencies. The term preparedness, as used below with respect to the Commonwealth, incorporates this definition.
- The Role of Risk Assessment in Homeland Security Planning. The Federal government, including DHS, has endorsed the use of "risk assessment" as a critical element of homeland security planning, and has clearly articulated that it

A(ix)[5] For further definitions of these terms, see Homeland Security Presidential Directive-8.

will, in establishing the National Preparedness Goal, "establish measurable readiness priorities and targets that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters and other emergencies." HSPD-8, ¶ 6. Within this framework, DHS is now in the process of working with other stakeholders to develop a range of "all hazard" scenarios for use in homeland security risk planning and establishing specific "tasks" needed to address these priority scenarios. The Commonwealth and its local governments can and should review these scenarios and utilize them as tools to assess their own vulnerabilities and develop their own strategies.

- <u>Federal Grant Funding Tied to Adoption of State Strategies</u>. The President has directed that the Federal government shall, to the extent permitted by law, predicate the provision of Federal preparedness grant assistance to states on "adoption of Statewide comprehensive all-hazards preparedness strategies." HSPD-8 states that such state "strategies" should be consistent with the National Preparedness Goal, should assess the most effective ways to enhance preparedness, should address areas facing higher risk, especially to terrorism, and should also address local government concerns … ."
- <u>Preparedness Requires Performance Measures</u>. Finally, HSPD-8 states that the National Preparedness Goal will establish not only "readiness metrics," but "a system for assessing the Nation's overall preparedness to respond to major events, especially those involving acts of terrorism." As states and localities play a critical role in meeting national preparedness goals, establishing performance measures for these non-federal capabilities is critical to overall preparedness.
- <u>Responding to Federal Alert Levels</u>. The Federal government has established a detailed level of alert procedures. The Commonwealth must have a procedure in place to respond to an increased Federal alert level. At the same time, given the significant degree of critical infrastructure in Virginia, the Commonwealth must have a procedure to independently raise its alert levels to protect its citizens and infrastructure without relying on a change in the Federal alert level.

C. <u>Performance measures must be "living and breathing</u>." Performance measures must be periodically reviewed and updated to adapt both to changing threats, consequences, and vulnerabilities and to changing Federal standards of homeland security for states and localities (some of which are utilized as criteria for providing funding to states and localities).

D. <u>Performance measures must be shaped for the Commonwealth and its local governments as well as for critical infrastructure, industry, and our citizenry</u>. Performance measures undoubtedly will vary from one level of government to another and one industry to another. There is no "one size fits all." Local governments will face different types and degrees of risk, and not every local government will be able to have in place a capability to guard against the full range of possible threats, including the range of high priority threats identified by DHS. This would be neither prudent nor cost-effective.

The performance measures recommended in this report are for the Commonwealth's state government (hereafter, the "Commonwealth) and its local governments. While the state is divided into regions for various administrative purposes, it is the province of local governments—with their legal authority, functions, budgets and personnel—to prepare for emergencies, declare states of emergency, request assistance and resources, and manage local emergencies.

In the public health arena, the picture is somewhat different. The Commonwealth's designated regions for public health purposes have some capability of their own and do play a role in emergency preparedness. It is therefore important to understand and measure the performance of the Commonwealth's regional public health capability.

E. Numerous existing performance measures should be utilized as appropriate. The Federal government, numerous states, and quasi-public or public standards bodies have created performance standards and measures for various aspects of homeland security and emergency preparedness. These include federally-mandated rules for nuclear reactors and local governments in regions where they are situated, Federal grant criteria that restrict eligibility for and use of funds, and private standards bodies that establish self-accreditation mechanisms in such areas as state and local emergency management.[6] In developing homeland security performance measures for the Commonwealth, we have recognized that:

1. Some state functions are governed by Federal law and grant conditions and criteria, and these rules may provide sufficient measures of performance in some areas (but leave gaps in others);
2. Existing standards developed by expert bodies may provide useful benchmarks that the Commonwealth should utilize for its own self-measurement (rather than developing altogether new standards covering the same ground); and,
3. Standards utilized by other states and localities offer useful elements that can be drawn upon and adopted to Virginia's circumstances. In effect, the Commonwealth will utilize a "system of systems" of standards that draws as appropriate on elements of the existing standards in assembling an overall "enterprise" set of measures against which the Commonwealth's performance should constantly be measured.

F. Performance Measures should be as objective as possible and focus on important indicators of performance. Performance measures are a method of collecting, analyzing, and reporting information in order to track resources used, work produced, and attainment of desired goals. In the ideal world, we would be able to track success by reference to societal "outcomes" of our preparedness policies (i.e., what public benefits have been derived from the Commonwealth's actions). In other words, have the Commonwealth's preparedness capabilities in fact reduced its vulnerability to homeland security threats and natural disasters? Thus, we could measure success by the number of homeland security or emergency "events" that occur and societal costs that

A(x)[6] In particular, the National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (2004) ("NFPA 1600 Standard") warrants careful consideration by the Commonwealth and its local governments.

result. While this approach is useful where relevant, the reality is that there are few objective measures that exist and they do not tell the entire story. Measuring how many events have occurred and their social costs does not necessarily correlate to how prepared we are for such events, which can vary in nature, size, location, and scope.

Thus, performance measures measure not only societal "outcomes," but also the effectiveness of the government's capabilities in a given area – here, preparedness capabilities. This type of measurement focuses on "inputs" into government capabilities (agency resources, plans, personnel, and the like), the "outputs" of such capabilities (i.e., how many hospital beds are provided during an emergency), and the efficiency of government response (how quickly or broadly are such capabilities provided – i.e., how quickly are alleged incidents responded to, etc.).[7] Indeed, the bulk of the performance measures suggested below relate to capabilities rather than outcomes. However, it also should be recognized that these "capability" tools may not, in the real world, necessarily fully correlate with reduced vulnerability. We may, for example, enhance capabilities in some areas only to find that other areas then become targets of opportunity for terrorists.

Furthermore, it should be recognized that the best performance measures are objective and quantifiable. While we have strived for this goal, there are difficulties in achieving it today. The new nature of the homeland security function makes it difficult to quantify performance in numerous areas at this time. For example, how many hospital beds do we need in a relevant geographic area? There are no clear answers to this today. The task force lacks sufficient information to form a judgment, and leaves further quantification to experts and to the development of more experience in this area. In addition, as a sign hanging in Albert Einstein's office at Princeton University said: "Not everything that counts can be counted, and not everything that can be counted counts." Thus, we must take this useful advice into account and avoid reliance on easily quantifiable measures simply because they are quantifiable. How quickly the Commonwealth processed incident reports may be readily observed but may not be an adequate gauge of our preparedness.

Thus, the performance measures below are mostly non-quantifiable in nature and are designed instead to focus on the areas where measurement is warranted. We have left it to experts in state government to develop more precise and quantifiable measures of these areas in the months and years to come.

G. Performance measures should be realistic and established with relevant time horizons in mind. Setting enterprise-level performance measures must take into account the realities of constrained budgetary and personnel resources as well as legal and governmental processes. It would make little sense to establish a set of performance measures, for example, that are unachievable due to the enormous resources required. Thus, measures must be established that are attainable in the short, medium, and long

A(xi)[7] For a useful overview of performance measures, see Guide to Performance Measure Management, Texas State Auditor's Office, 7-8 (1999).
A(xii)

term. Many of the capabilities set forth in this report are not fully in place or operational today; they are works in progress or likely to be established over the next few years.

H. Performance measures should measure not only what capabilities are "put in place," but also the degree of implementation and effectiveness of the capabilities. Understandably, a major focus of performance measures, especially in this initial period of development, is on assessing whether the core capabilities are put in place. At the same time, however, it is important to capture and measure, to the extent possible, not only the establishment of such capabilities, but also whether they are operational and effective. Undoubtedly, as discussed below, exercises will be part of this effort, especially in the area of measuring response to incidents. But other measures also may be necessary in the areas of prevention and detection. As time goes by, and more capabilities are put in place, implementation and execution will become the focus of measuring preparedness.

3. Identifying Areas for Performance Measures

In order to assist the Commonwealth in developing performance measures, we have identified particular capability areas and sub-areas that should, in our view, be measured. The list is not meant to be exhaustive but rather exemplary. We suggest key measurements in each capability area that should be reviewed by experts and, subject to their judgment, made more quantifiable or detailed as appropriate.

With these considerations in mind, the following are the subject areas in which performances measures are appropriate relative to homeland security capabilities:

A. General Capabilities:

1. Laws and Authorities
2. Accountability and Organization
3. Planning/Risk Assessment Function
4. Budgetary Transparency and Accountability
5. Grant Functions (Grantor and Grantee)
6. Intergovernmental Relationships
7. Continuity of Government

B. Specific Functional Capabilities:

- Communications
- Critical Infrastructure
- Emergency Response
- Health and Medical Preparedness
- Information Sharing
- Information Technology Security
- Law Enforcement and Criminal Justice

- Mutual Aid
- Private Sector Preparedness
- Public Awareness
- Recovery
- Training and Exercises
- Transportation

C. Support Capabilities - The Focus on Training:

In each of these areas (general and specific functional capabilities), it is important to assess whether the Commonwealth and its localities have in place sufficient supporting capabilities, as reflected in:

1. Plans, procedures and strategies;
2. Funding (whether from budgeted funds, grant assistance or otherwise);
3. Assigned personnel; and
4. Training.

Given the relatively new and developing nature of the homeland security and preparedness capability, it is particularly critical to fund training at all levels of government. The presence of adequate and ongoing training – has the government unit assessed its training needs, identified personnel requiring training, secured resources for it, and proceeded to conduct the training – is a critical performance measure.

Thus, whether explicitly mentioned or not, each of the performance measures set forth below should be assumed to include, as a sub-element, these support capabilities.

4. Commonwealth Preparedness Capabilities and Performance Measures

A(v) Below we set forth recommended performance measures. We have crafted each of these measures in terms of a general question that is designed to serve as an overall introduction to the particular subject and capture the overall performance objective. The more specific "sub-elements" that follow each question comprise the performance measures designed to answer it.[8] Finally, where appropriate, we have provided a comment section designed to illustrate key challenges and issues and steps the Commonwealth has taken in various areas.

A(xiii)[8] While we recognize that performance measures generally are phrased as declaratory statements rather than questions, the distinction is not a substantive one. These questions can easily be rephrased.

A. General Capabilities and Measures

I. Laws and Authorities

Do the Commonwealth and its local governments have in place the necessary laws, regulations and other measures needed to provide the broad-ranging authority necessary to meet the Commonwealth's preparedness goals?

Sub-Elements:

- Do the Commonwealth and its local governments have in place an effective and institutionalized process to periodically evaluate existing laws, regulations, codes, and other authorities to determine whether adequate and flexible authority exists to meet preparedness goals and accommodate homeland security developments?
    - Have the Commonwealth and its local governments addressed the legal "gaps" identified through such a process to date?
- Does the Commonwealth's process for addressing legislative "gaps" bring together all stakeholders and take into account the full range of potential impacts of such legislation, including budgetary costs, burdens on the private sector and the public, and issues concerning privacy and the treatment of proprietary private sector information?
- Does the Commonwealth have a long-term "gap" strategy to address the need for legislative and regulatory revisions?
- Do Commonwealth agencies and entities that have the authority to conduct emergency operations have authority to take action prior to an event to mitigate the occurrence or recurrence of the event?
- Does the Commonwealth's evaluation of exercise results (see Performance Measure VII, "Continuity of Government," below) consider the need for and impact of changes to laws, regulations, and or legal authorities?

Comment: The Secure Commonwealth Panel and the Governor's Office of Commonwealth Preparedness ("OCP") have together played critical roles in identifying and shaping legislation to fill "gaps" in preparedness authority. However, neither the Panel nor OCP are institutionalized entities; and both, created by executive order of Governor Mark Warner, will expire at the end of his term. Accordingly, a permanent process should be developed to review state laws and regulations pertaining to security and preparedness on an ongoing basis. See also the Comment to Performance Measure II, "Accountability and Organization," below.

II. Accountability and Organization

Do the Commonwealth and local governments have clearly established lines of authority for "all hazard" preparedness that specifies which units of government and individual positions are responsible for particular functions,?

Sub-Elements:

- Does the governmental entity have a unit or individual in charge of coordinating all of the elements of the multidisciplinary, multiagency preparedness function?
- Does each agency or other preparedness function at the state and local level have written protocols in place for cooperation with other governmental entities?
- Does the allocation of authority for homeland security functions reflect an efficient, effective, and equitable balance of responsibility and authority among the government entities?

Comment: The Commonwealth's experience dealing with emergency situations in recent years has highlighted the critical need for clear lines of authority and accountability not only for such events, but also for the forward planning needed to deter, prepare for, and recover from such unfortunate events. The role of the OCP has been vital in shaping a holistic approach to preparedness for Virginia. The members of this task force find that there is a vital need for a central coordinating entity for long-term security and preparedness in the Commonwealth. It therefore is the recommendation of this task force that OCP, which currently exists by virtue of executive order that will expire in accordance with the terms of such order, should be made permanent by the General Assembly during its next session.

The task force recommends that the General Assembly provide the coordinating office it creates with broad authority to manage and coordinate the homeland security function for Virginia. The office should also be given responsibility to identify and fill legal gaps in authority, prepare and address budgetary needs (working in coordination with other state departments and agencies), allocate Federal grant assistance where such decisions are discretionary (or supervise its allocation by responsible state departments or agencies), and work with the Federal government, other states, and local governments to develop and implement a preparedness strategy for the Commonwealth.

The task force recommends that the continued need for a Governor-appointed panel for security and preparedness also should be considered by the General Assembly. While there is considerable merit and utility to this approach, especially in the formative period when it is important to bring all stakeholders to the table and shape the initial strategy, at some point the panel's functions should be institutionalized whether through OCP or a separate advisory board.

III. Planning/Risk Assessment Function

Does the Commonwealth, or local government, have a plan and planning mechanism that reasonably addresses its "all-hazards" preparedness goals (including prevention, response, and recovery)?

Sub-Elements:

- Is the plan and its proposed elements, priorities, and resource allocations based on a reasoned assessment of overall risks that takes into account possible threat scenarios (including the planning scenarios recently promulgated by DHS), the likelihood that such scenarios could occur in the relevant geographic area, the magnitude of such incidents, and potential consequences and costs?

  - Has the governmental unit identified potential hazards and inventoried facilities or locations where risks exist?
  - Does the planning process and resulting plan appropriately utilize the hazard identifications and risk assessment methodologies set forth in the National Fire Protection Association 1600 Standard on Disaster/Emergency Management and Business Continuity Programs (2004) ("NFPA 1600 Standard")?
  - Has the Commonwealth or local government undergone the DHS Office of Domestic Preparedness' Homeland Security Assessment?[9]
  - Do all local governments have mitigation plans that meet the standards of the Federal Disaster Mitigation Act of 2000[10], which established a requirement that local governments have mitigation plans in order to be eligible for Federal grant funds, including the Hazard Mitigation Grant Program?
- Did the government entity consult with all relevant stakeholders in developing its plan, including governmental, police and law enforcement, fire, emergency response, transportation, health and medical, military affairs, and the private sector?
- Is the plan periodically reviewed and revised to take into account changing DHS and other Federal standards, planning scenarios, vulnerabilities, resources, and other factors?
- Does the government entity have the appropriate personnel, budgetary resources, and analytical tools to properly conduct efforts under A in Section 2—"Key Considerations in Shaping and Measuring Preparedness Capabilities"— above?

Comment: Population size and concentration is certainly a relevant consideration in risk-based planning, including, for example, in evaluating consequences of potential threat scenarios and allocating resources to address these threats. See HSPD-8 (directing Federal departments and agencies, in providing first responder preparedness assistance, to base allocations on "assessments of population concentrations, critical infrastructures, and other significant risk factors … .").

Members of the task force recommend that the Commonwealth develop its security and preparedness plan and allocate resources on the basis of an assessment of "risks" and not on the basis of a pre-ordained or automatic formula based on population. Artificial and non-risk based formulas should not be utilized by the Commonwealth in preparedness planning.

[9] See http://www.shsasresources.com.
A(xiv)[10] Pub. L. No. 106-390, 114 Stat. 1552.

IV. Budgetary Transparency & Accountability

Does the Commonwealth or local government have the budgetary resources to meet identified preparedness needs?

Sub-Elements:

- Does the unit of government have:

  - Transparent records of its past total spending on preparedness and funding sources;
  - A projected budget for the future – at least two years, together with a written list of funding sources, when known; and
  - A mechanism for tracking the spending and use of Federal grant funds?

- Have all possible funding sources been identified, including the use of tax benefits?

Comment: The availability of Federal grant assistance is generally known only a year in advance. Thus, budgets beyond one year would be somewhat notional but are helpful to encourage long-range planning by government units. However, where possible, it is important to have predictable funding streams (whether through multiyear Federal grants or multiyear Commonwealth appropriations of funds).

V. Grant Functions (Grantor & Grantee)

Has the government entity expeditiously, reasonably, and transparently allocated and/or expended grant funding related to its preparedness functions from the U.S. government and other sources?

Sub-Elements (Commonwealth):

- Has the Commonwealth developed one or more fair, reasonable, and transparent mechanisms for distributing Federal grant assistance to local governments, and has it utilized this mechanism in practice?
- Does the Commonwealth take into account the performance of local governments under the performance measures noted herein in distributing such funding?
- Does the Commonwealth utilize the risk-assessment methodologies in distributing funding rather than solely relying on population or other criteria? (see the Comment on Performance Measure III, "Planning Risk Assessment Function," above)
- Does the Commonwealth have an adequate capability to review and measure the performance of local governments in taking their performance into account in distributing funding?

Sub-Elements: (Commonwealth and other local government recipients of grant funds):

- Do local governments that receive grant funding disperse such funding efficiently and expeditiously?
- Have local governments that have sought grant funding for the acquisition of equipment funded the resources necessary for training in the use of such equipment?
- Does the Commonwealth or government entity have a mechanism in place to address identified but unfunded needs and to ensure appropriate funding in the future?
- How many local governments did and did not receive grants in each of the last three years? Why did some governments not receive funding, and what is the consequence of the lack of support?

Comment: While we have been unable to quantify with precision how much of the Commonwealth's preparedness funding is from Federal grant assistance (such data is not readily available at this writing), it is clearly the case that Federal grants are the primary source of such funding. Accordingly, it is critical that the Commonwealth and its local governments be accountable for the distribution and use of such important funding. The Federal grant assistance criteria change from time to time, and vary from one functional area to another. Nevertheless, it is vital that the Commonwealth maintain its own disciplined approach to exercising its discretion, where it exists, to allocate funding in the State within the parameters of Federal grant criteria. Such methodologies should be in written form and consistently applied (as they are in the health area today).

As a significant percentage of funding is for equipment at the local level, it is equally important that localities have assessed training needs with respect to such equipment and funded and performed such training. It is of little utility to maintain equipment that will go unutilized in an emergency.

VI. Intergovernmental Relationships

Do the Commonwealth and its localities have the intergovernmental relationships necessary to ensure Virginia's preparedness?

Sub-Elements:

- Have the Commonwealth and localities forged strong intergovernmental relationships in critical preparedness mission areas (including, among others, intelligence and warning, transportation security, critical infrastructure protection, and public health) that can facilitate the cooperation, coordination, and collaboration necessary to ensure a safe, secure and prepared Virginia, including:
  - Vertical relationships—relationships between Federal, state and local entities;
  - Horizontal relationships—coordination between similar state or local government entities; and
  - Geographic relationships—relationships with bordering states.

    - Do the preparedness plans, funding mechanisms, policies, and procedures of the Commonwealth and its localities contain elements? designed to foster intergovernmental cooperation, coordination and collaboration? Do the Commonwealth's preparedness goals, plans and strategies include intergovernmental or interjurisdictional elements?
    - Do the procedures and protocols on intergovernmental activities reasonably cover activities needed for all elements of preparedness (prevention, preparation, response, and recovery), including:
        - preparation and implementation of preparedness plans and strategies;
        - sharing of intelligence and other relevant information (including local vulnerabilities); and
        - areas where mutual aid plans and procedures are put in place.
    - Are appropriate mechanisms for intergovernmental communications established?
        - Are there common protocols and designated primary and secondary points of contact known to and understood by relevant units of government?
        - Are there regular and ongoing communications between these entities?
- Has the Commonwealth, and its local governments, developed, articulated and implemented a shared vision with respect to intergovernmental relationships? Do governmental entities in the Commonwealth:
    - routinely identify specific and timely opportunities for intergovernmental action and innovation in support of their own preparedness goals and those of other relevant governmental units;
    - look at issues holistically;
    - build on previous successes in cooperation and collaboration for longer-term collaborative efforts; and
    - routinely identify main stakeholders, potential partners, and other affected parties and collaborate with these entities; and
    - routinely incorporate intergovernmental relationships in their day-to-day operations?
- Does collaboration encompass all phases of the goal—planning, funding, approval, implementation, training, exercises and maintenance?

<u>Comment</u>: There are often strong governmental tendencies (institutional and cultural) and citizen desires to maintain the independence and prerogatives of existing governmental entities. Efforts to enhance coordination and collaboration must seek to re-orient existing entities and structures to ensure effective intergovernmental relationships are integrated into and become part of each organization's goals, missions, and structures.

The National Capital Region ("NCR") presents a unique challenge for coordinating regional and intergovernmental planning, cooperation, preparation and response for the multiple government entities responsible for its over four million citizens and institutions. The NCR is comprised of the leadership of the District of Columbia, State of Maryland, and the Commonwealth of Virginia. Virginia has several representatives on the NCR's Senior Policy Group.

The NCR has made significant progress in meeting the complex challenges of risk management, homeland security, and preparedness and has set an example for regional planning and coordination and responsiveness. This regional, intergovernmental coordination resulted in an NCR better prepared and more secure with a needs-based regional strategy for risk management, improving preparedness, and addressing security.

VII. Continuity of Government

Is there a written plan to ensure the continuity of key governmental functions and facilities at the Commonwealth and local level during a homeland security incident or natural emergency?

Sub-Elements:

- Are there laws, regulations, or procedures in place for:
  - the declaration of a state of emergency; and
  - succession of key executive branch and legislative personnel?
- Has the unit of government identified the critical, time-sensitive records and data ("critical data"), and government functions and processes that must be maintained during emergencies;
- Is there a written plan sufficient to ensure the continuity of critical records and government functions during an emergency?
- Do the continuity plans provide for their periodic review to ensure that they remain current?

Comment: The Commonwealth has had plans in place for a number of years that have evolved over time, including plans for high level succession planning. More steps are needed to ensure continuity of governmental functions and critical records at the local government level.

B. Specific Functional Capabilities & Performance Measures

VIII. Communications

Does the Commonwealth have sufficient, reliable and interoperable communications systems (internally and with the Federal government and other states and entities as appropriate)?

Sub-Elements:

- Are there redundant communications systems in place should one system fail?
- Are the Commonwealth's systems and those of its local governments inter-operable with one another and do they allow adequate and reliable communication between each other and with Federal officials?

- Do the Commonwealth and its local governments have reliable procedures to notify officials and emergency response personnel potentially impacted by an actual or impending emergency?
- Is the Statewide Agencies Radio System ("STARS") program on schedule for completion? What percent/number of local governments will participate in STARS?
- Do the Commonwealth and its local governments have the capability to meet all elements of their emergency response plans?
- Are written protocols, processes and procedures in place at the state and local level for communications during emergencies?
- Does the Commonwealth have in place an adequate Emergency Alert System ("EAS") that can notify those people or areas potentially impacted by an actual or impending emergency?

Comment: By Executive Order 28 (2002), Governor Warner established a program to develop the STARS system of integrated radio and wireless data communication for state agencies engaged in public protection and safety and for the mutual aid needs of state and local law enforcement agencies. The STARS program recognizes the need for a shared, statewide, public safety-grade radio system that includes law enforcement mobile data, and facilitates interoperability between state and local police communications systems at the city or county level. STARS will replace the existing analog communications system used by the Virginia State Police and other state agencies with a VHF digital high-band trunked system that integrates radio and wireless data communications. The Commonwealth has entered into a contract for the procurement of the system and it is expected that the system will be partly operational in 2005 and fully operational by 2009.

IX. Critical Infrastructure

Are adequate protections in place for all portions of the Commonwealth's infrastructure identified in the National Asset Database as "critical"—including utilities, nuclear facilities, commercial assets, and others?

Sub-Elements:

- Are all potential critical infrastructure sites identified by the units of government in which they are located?
- Has a buffer zone protection plan ("BZPP") been established for each identified structure or location?
- Has the BZPP been exercised and have security audits been conducted in order to ensure feedback?
- Is there a plan to handle multiple site incidents?
- Are the consequence zones or interdependencies of any particular site cross-jurisdictional? If so, are mutual aid measures in place?

Comment: Under the U.S.A. Patriot Act,[11] the term critical infrastructure refers to those "systems and assets (resources), whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety or any combination of those matters." The DHS Protective Security Division builds the National Asset Database from thirteen sectors and four key resource areas. The sectors include: agriculture and food; water; public health; emergency services; defense industrial base; information; telecommunication; energy; transportation; banking and finance; chemical and hazardous materials; postal and shipping; and national monuments and icons. DHS also utilizes the following four key resource areas: nuclear power plants, dams, government facilities, and commercial assets.[12]

The BZPP program provides funding to reduce vulnerabilities of critical infrastructure ("CI") and key resource ("KR") sites by extending the protected area around a site, thus creating a further protection in the surrounding community. The DHS Information and Analysis and Infrastructure Protection (IAIP) division, in participation with state and local officials, reviews vulnerability assessments to identify security needs. The BZPP program is administered by staff assigned to the Security & Emergency Management Division (Transportation Protective Security) of the Virginia Department of Transportation, in direct support of the Office of Commonwealth Preparedness. The program involves liaison with local law enforcement and owners/operators of CI/KR sites throughout Virginia, in order to continue to safeguard our nation and minimize the potential for a terrorist attack. The BZPP helps local authorities assess current vulnerabilities at identified critical infrastructure and key resource sites, and develop and implement plans to increase the level of protection, while acting as a deterrent and prevention mechanism of possible terrorist threats or incidents. In developing these plans, responsible jurisdictions review and assess ways in which they can work with relevant Federal, state, local, tribal, and private sector agencies to coordinate their prevention activities.

X. Emergency Response

Do the Commonwealth and its local governments have the capability to oversee and coordinate a timely and comprehensive response and recovery plan for man-made and natural disasters?

[11] Pub. L. No. 107-56, 115 Stat 272. See also Homeland Security Presidential Directive – 7 (specifically defining and enumerating the critical infrastructures in the United States) (see http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html).

[12] See also Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection (Oct. 1997). See also Homeland Security Presidential Directive – 7 (specifically defining and enumerating the critical infrastructures in the United States)
(see http://www.whitehouse.gov/news/releases/2003/12/20031217-5.html).

Sub-Elements:

- Have the Commonwealth and its local governments been accredited by the Emergency Management Accreditation Program ("EMAP")?
- Have local governments conducted self-assessments using the Local Capability Assessment for Readiness ("LCAR") self-assessment instrument and used the results to strengthen capabilities?
- For the Commonwealth—How many of Virginia's local governments have been accredited under EMAP and/or self-assessed under LCAR (in percentage and absolute terms)?
- What departments and agencies within the Commonwealth are designated as emergency responders? What level and type of emergencies will warrant a request for assistance from the Federal government (e.g., National Guard) and private organizations?

Comment: While the EMAP accreditation process is effective, the process is expensive and lengthy and hence may not be a viable alternative for localities in the absence of grant assistance. Thus, task force members recommend that LCAR self-assessments are a reasonable alternative to the EMAP accreditation approach.

XI. Information Sharing

Does the Commonwealth have access to all relevant information, including intelligence from the Federal government and a fusion process to evaluate and disseminate relevant information and intelligence to State and local entities and the private sector?

Sub-Elements:

- Has the Commonwealth identified all key sources of relevant information, including sources within the private sector?
- Have policies and protocols been developed for gathering and sharing of information?
- Have state and local personnel been trained to recognize relevant information, gather it appropriately, and disseminate it in a timely fashion?
- Has the Commonwealth identified all entities, including within the private sector, to whom relevant information should be disseminated?
- Have appropriate policies and protocols been developed to ensure the widest possible access to, and sharing of, information consistent with the need to protect classified information, sensitive law enforcement information, and privacy and due process rights?
- Do the Commonwealth's fusion process/Fusion Center and Emergency Operations Center ("EOC") have clear missions and strategic plans?
    1. Are the Commonwealth's fusion process/Fusion Center and EOC adequately and appropriately staffed, including by personnel from agencies with relevant informational needs and capabilities?

2. Do the Commonwealth's fusion process/Fusion Center and EOC maximize participation by, and information sharing with, state and local government entities?

- Does the Commonwealth have the capability to communicate and store classified information in compliance with Federal standards?

Comment: The Virginia Fusion Center has been established to address many of these issues. The concept of the Virginia Fusion Center is to bring key critical response elements together in a secure, centralized location so that information and resources can be shared in order to provide a well-orchestrated and coordinated intelligence function. The information will be collected, prioritized, classified, analyzed and disseminated in order to better defend the Commonwealth against terrorist threats and/or attack. The Virginia Fusion Center should be operational in the autumn of 2005. It is the intent that all relevant terrorism information and intelligence be centralized and directed or legally mandated to be processed through the Center.

At the same time, however, it should be recognized that the Fusion Center cannot provide all needed capability or be a substitute for maintaining necessary Commonwealth functions of detection, investigation, surveillance, and others related to identifying and preventing potential homeland security threats.

XII. Information Technology Security

Does the Commonwealth have an effective information technology ("IT") security plan?

Sub-Elements:

- Is there an agency or person responsible for Virginia's IT security? Is that agency or person in contact with relevant private sector entities so that threats to each are shared quickly and appropriately?
- Are reports of cyber attacks in the Commonwealth tracked, and is a responsible agency in charge of addressing them? Have the number of reports increased or decreased in the last year? Is there an agency within the Commonwealth that reports cyber incident statistics to the Software Engineering Institute (SEI), and are there collaboration opportunities that exist between the Commonwealth and SEI?
- Have rules and procedures been put in place to facilitate the supply of such information by the private sector to the Commonwealth and, as appropriate, its local governments? Are policies and procedures in place to ensure that all information technology systems (the Commonwealth and its local governments) receive critical security updates in a timely manner?
    - Is there a program that provides regular testing of information technology systems to audit and report whether they have received critical security updates?
- Have rules and procedures been put in place by the Commonwealth and its local governments to require the assessment and mitigation of risk in all information technology systems that store, process, and transmit sensitive data?

    - Do such policies and procedures include requiring acceptance of any residual risk by Executive management?
    - Do such policies and procedures require that any and all new information technology systems be reviewed prior to deployment to ensure that they meet Commonwealth technology architecture standards, including security standards?
- Have all Commonwealth personnel who use information technology resources received basic security awareness training?
    - Have Commonwealth personnel with additional information technology responsibilities received advanced security awareness training commensurate with their responsibilities?

Comment: In this area, like others, it is critical to forge a partnership between government and the private sector. For businesses to share information about cyber attacks with the Commonwealth, there must be a sufficient degree of trust involved—i.e., is the Commonwealth's protection of private entities against cyber attack sufficient to encourage these entities to share such information with the State government? Thus, it is imperative to establish modalities for this type of information sharing that limit access to such information to those in State government with a "need to know" and take steps to ensure this information is adequately safeguarded against inadvertent release.

XIII. Law Enforcement & Criminal Justice

Does the Commonwealth have an effective capability to develop and utilize all available information to deter, detect, and prosecute individuals and groups that cause homeland security threats?

Sub-Elements:

- Does the Commonwealth have the means to gain access to all relevant intelligence from the Federal government—classified or otherwise—and all other relevant information (developed in-state or otherwise), and appropriately fuse, evaluate, and disseminate such information to appropriate Commonwealth and local personnel as needed? (See Performance Measure XII**,** "Information Technology Security," above for details).
- Does the Commonwealth have the capability to deal rapidly with "tips" and potential threats, including expedited analysis and investigation, real time sharing of information with Federal authorities and others as appropriate, and development of quick responses?
- Does the Commonwealth and its local governments, and police and other law enforcement personnel, have in place procedures and protocols for acting to deter and detect homeland security threats?
    - Are the protocols and procedures coordinated and integrated among all affected entities, including those that have not participated in homeland security matters in the past?

  - Does each participating partner understand its mission and requisite operational purpose?
- Do the Commonwealth and its local governments have the trained personnel and funding needed to carry out such activities?
  - Are agencies required to provide training for their personnel, and is training identified as a priority for both preparedness and budgetary planning purposes?
  - Are adequate funding streams in available to meet training needs? (recognizing that Federal grant assistance generally *cannot* be used *in place of* State funds but may only supplement State funds)
- Does Virginia's judiciary have in place procedures and protocols to deal with sensitive information in carrying out prosecutorial functions relative to homeland security?

<u>Comment</u>: The task force understands that certain law enforcement entities, including the Virginia Sheriffs, in the past have received Federal grant assistance that has enabled them to accomplish many of the objectives set forth above. With this funding, the Sheriffs' Association established a Terrorist Information Coordinator that played a valuable role in facilitating communications between law enforcement personnel. However, funding under that grant will not be available after August 2005. The task force therefore recommends that the Commonwealth make available funds in order to continue the progress of the Virginia Sheriffs and consider bringing the program under the auspices of the Virginia Fusion Center.

Similarly, the task force recommends that the Commonwealth avoid stovepiping with respect to law enforcement intelligence and information sharing because the costs can be significant. In this regard, communication between relevant law enforcement entities in the Commonwealth should be improved to ensure various intelligence gathering and dissemination mechanisms are properly utilized and coordinated.

XIV. <u>Mutual Aid</u>

Have the Commonwealth and its local governments utilized mutual aid agreements in their security and preparedness plans to maximize use of available resources?

<u>Sub-Elements</u>:

- Do the Commonwealth and local governments take the availability of assistance from other jurisdictions and entities into account in developing preparedness plans?
- Does the Commonwealth have mutual aid agreements in place with other states to help provide "surge" assistance in the event of a homeland security incident or natural disaster?
- Is the Commonwealth a participant in the nation-wide Emergency Management Assistance Compact ("EMAC")?

- How many local governments within the Commonwealth have mutual aid agreements in place with other governmental units and private sector businesses (in percentage and absolute terms)?
- Are the Commonwealth and its local governments aware of existing mutual aid agreements in place relevant to their territorial jurisdiction that would be activated in the event of an emergency?

Comment: The Commonwealth was one of the first members of the nationwide Emergency Management Assistance Compact that includes most U.S. states and territories and has in fact received as well as provided EMAC assistance. Most of Virginia's 140 local jurisdictions are signatories to the Statewide Mutual Aid System, which has successfully been used in disasters.

XV. Private Sector Preparedness

Is the role of the private sector integrated into state and local security and preparedness plans? Do private sector entities in the Commonwealth have in place plans and processes to ensure their "all-hazards" preparedness?

Sub-Elements:

- Do private sector businesses in Virginia have a process, adequately funded and supported by senior management, to ensure the necessary steps are taken to identify potential risks to their facilities and the impact of potential losses, establish appropriate safeguards (physical and information security, etc.), maintain viable recovery strategies and plans, and ensure continuity of services?
    - Do such "continuity of business plans" consider the specific areas set forth in the NFPA 1600 Standard, Annex A, A.5.7.2.5?
- Do private sector businesses engage in personnel training and plan testing and maintenance, and undertake self-assessments of their preparedness?
- Have the Commonwealth and its local governments identified key private sector businesses critical to ensuring ongoing continuity of basic services to the citizenry and worked with those businesses to ensure continued service in case of a disaster or emergency?
    - Does the Commonwealth promote and participate in joint training and exercises with the private sector?
- Have the Commonwealth and its local governments worked cooperatively with the private sector to: 1) identify private sector resources that can be used in responding to specific emergencies, and 2) agree upon and put in place mechanisms to ensure access to those resources in the case of such emergencies?
- Have at-risk industries such as utilities, water treatment facilities, and chemical and nuclear plants established voluntary codes that specify preparedness and precautionary measures?
- Does sufficient sharing of information occur between the Commonwealth and the private sector regarding critical preparedness missions, and are there steps in place to enhance and improve such information sharing?

- Do private sector businesses in the Commonwealth have sufficient awareness of the state's Emergency Response Plan and the steps businesses are advised to take in connection with different terrorist threat conditions? (See http://www.commonwealthpreparedness.virginia.gov/SecureVa/vathreat.cfm.)
- Do private sector entities have effective information technology security plans and protocols for sharing information concerning IT incidents with the Commonwealth and its regions and localities? See Performance Measure XII, "Information Technology Security," above.

Comment: The private sector should be treated as an integral component of the Commonwealth's preparedness planning and response. The private sector must be a partner in every aspect of preparedness planning, including information sharing and participation in exercises and recovery strategies. Private sector firms bring many specialized skills, unique talents, and resources to the table that should be harnessed by the public sector for emergency situations. Such capabilities as electric power line crews, fiber optic repair teams, fuel transport, specialized construction, and excavation can be very useful in responding to an event.

Relevant processes and metrics exist in many Commonwealth industries (especially those that qualify as critical infrastructure and are subject to Federal or State regulation) and should be utilized where appropriate.

XVI. Public Awareness & Warning

Is the public knowledgeable about state and local preparedness goals? Are there mechanisms in place by which the public receives timely notification about emergency situations, what emergency actions should be taken, and the state and local response and recovery plans?

Sub-Elements:

- Do the Commonwealth and its regional and local governments have procedures and protocols for disseminating information to the public, the media, the private sector, and volunteer organizations with respect to each of the following:
    - the prevention of emergency events;
    - what steps to take if an emergency occurs; and
    - what to do during the recovery phase?

- Do these plans take into account and balance:
    - Differences between the types of homeland security needs (prevention, preparedness, response, and recovery) and the different public groups and localities; and
    - Considerations of timing, potential public impact of announcements, the need to minimize panic, and the desire for full and accurate disclosure of material risks to the public?

- Do the Commonwealth and its regional and local governments have the public information capability (such as telephone hotlines, websites) to handle citizen inquiries on homeland security and emergency matters and the ability to expeditiously respond to inquiries?
- How many of Virginia's citizens are aware of the steps citizens are advised to take in connection with different terrorist threat conditions (as set forth at http://www.commonwealthpreparedness.virginia.gov/SecureVa/vathreat.cfm) and the need to develop an all-hazards family disaster plan and disaster supply kit?
- Does the Commonwealth have a plan to increase overall public awareness of its plans and the steps the public should take?
    - Does the Commonwealth have the capability (including public relations liaisons) and strategies in place to work with the media to educate the public on these issues?

Comment: Empirical evidence available to date suggests that improvement is warranted in the public awareness of the steps for citizens to take at different threat levels and to prepare themselves for all hazards. Accordingly, the need for a plan to improve awareness is built in as an element of the needed capability on public awareness. The Joint Information Center ("JIC"), which is set up in the event of an emergency, should improve public awareness. However, efforts must be made to evaluate the overall effectiveness of the Center and modify its mission and operating procedures when necessary.

XVII. Public Health & Medical Preparedness

Does the Commonwealth have the medical and healthcare related capabilities (trained personnel, medicines, health care facilities, and other resources of sufficient size, scope and numbers) to investigate, respond to, and contain a range of "all hazards" events that could harm public health?

Sub-Elements:

- Does the Commonwealth have in place the following capabilities, systems and capacities, including necessary funding, personnel and equipment:
    - Planning/Preparedness:
        - A statewide plan to address the public health effects of "all hazards" that encompasses the following elements:
            - identification and prioritization, on a risk basis, of the full range of potential public health events that could occur in the Commonwealth, including events involving mass fatalities;
            - the effective management of the public health aspects of such events and their aftermath and the expeditious and

coordinated delivery of critical health and mental health services, including:

- identifying clear lines of responsibility within State government for handling needed functions in such public health emergencies;
- developing State and regional plans for "surge capacity" for public health, healthcare and behavioral health responses to all such events, including emergencies involving mass fatalities; and
- plans for collaboration with hospitals, the medical community, behavioral health providers, long-term care facilities, outpatient facilities, homecare agencies, and other health providers and professionals in responding to such events.

- a statewide system for 24 hour/7 day a week notification and/or activation of the public health emergency response system;
- a system and directory of volunteers who can provide assistance in public health, healthcare and behavioral health responses to all emergencies;
- statewide plans and procedures for receipt and distribution of medications and supplies from the Strategic National Stockpile and plans at the State and local levels for the timely dispensing of antibiotics or vaccines to affected populations;
- corresponding all-hazard plans for the local health districts; and

- managing and counseling (as appropriate) individuals who suffer post-traumatic stress disorder, which is a typical response to events that involve mass fatalities.

- <u>Epidemiology/Early Disease Identification</u>

  - The capability and systems to:

    - receive and evaluate urgent disease reports, including ensuring legal authority to require and receive reports and investigate as appropriate;
    - assure the timeliness and completeness of reportable disease surveillance systems for outbreaks of illness;
    - maintain links with animal surveillance systems and the animal health community to facilitate identification and management of human diseases acquired from animals;
    - sufficient epidemiologic response capacity and capability to investigate and respond to infectious disease outbreaks, bioterrorism events, intentional or unintentional chemical exposures, radiologic events, and natural emergencies that impact the health of the affected population; and

        - guidelines for implementing isolation and/or quarantine procedures as appropriate and necessary for individuals or populations.

- Laboratory Capability & Response

    - The capability and systems for:

        - rapid laboratory testing, with appropriate confirmation of results, for samples linked to infectious disease outbreaks, possible bioterrorism events, and accidental or intentional chemical exposures;
        - rapid and safe transportation of samples to the laboratory for appropriate biologic or chemical testing; and
        - expedited communications between the State laboratory and the Virginia Department of Health, hospitals, other healthcare providers, and laboratories statewide for transmission of laboratory results.

- Communications/Information Technology

    - The capability and systems for:
        - notification of key stakeholders involved in public health or healthcare detection and response. including a 24 hour/7 day flow of critical health information;
        - redundant communications for public health and healthcare providers; and
        - coordination of communications and communications systems with all other emergency response agencies and organizations within the Commonwealth.

- Public Health Information

    - A plan for crisis and emergency risk communication and information dissemination concerning public health and healthcare issues;
    - Training of key State and local public health spokespersons in crisis and emergency risk communication principles and standards;
    - Coordination of risk communication planning (i.e. plans for communicating information to the media and the public during an emergency) with key State and local government and non-government emergency response partners;
    - Collaboration of Commonwealth public health entities with Virginia's non-health emergency management units not only through the Joint Information Center, but also with input from the Emergency Operations Center and the Fusion Center in order to assure coordinated communication with the media and public during any emergency event.

- Education and Training

    - Training for health department staff and healthcare providers in public health and healthcare emergency response to natural and man-made emergencies, including infectious disease outbreaks, terrorist events, chemical exposures, and radiological, nuclear, and explosive events. Training should include Incident Command, the National Incident Management System ("NIMS"), a DHS program that integrates practices in emergency preparedness and response into a comprehensive national framework for incident management, and the roles of all response agencies in responding to emergency events;
    - Coordination of training activities with all other State agencies involved in emergency response; and
    - Provision of access to necessary training to the broadest group of public health and private heath care providers, as well as other emergency responders (using newer technologies, where possible, to facilitate training).

Comment: To achieve the necessary level of public health planning, the Commonwealth needs to complete the preparation of its emergency operation plan ("EOP") and associated Emergency Support Function (ESF) 8—the health and medical response emergency support function; consolidate all existing plans (SNS, smallpox pre-event and post-event, pandemic flu, SARS, etc.) within the EOP; and incorporate additional disaster and emergency plans as appropriate.

While various Federal grants establish initial levels of surge capacity and related metrics (hospital beds per population size, etc.), there appears to be little empirical basis at present for identifying hard and fast levels of capability for the Commonwealth. Only continued exercises and experience will allow the development of more meaningful quantitative metrics for Virginia and its regions and localities. In developing these more measurable statistics, it also should be recognized that such metrics will likely change from one region to another (nationally and within states) and that a critical element is identifying statewide metrics that rely heavily on transportation and mutual aid for surge capacity.

It should be recognized that few if any jurisdictions are likely to have the range of capabilities noted above and that the Commonwealth, like other states, is now in the process of moving to acquire and make operational these types of capabilities.

Finally, as noted above, the public health capability of the Commonwealth has an emerging regional component that should be further developed and measured. The Virginia Department of Health ("VDH") has five regions for emergency planning and response (based on public health and healthcare planning and referral patterns) that are different from administrative regions utilized by the Virginia Department of Emergency Management and the State Police. The VDH effort includes a team of 5-6 people in each region as well as a hospital coordinator funded through Federal grants, that are involved in regional planning efforts and assisting health districts and hospitals in their regions. During emergencies, the regional teams assist the districts, hospitals, and VDH Central

Office in collecting information and providing additional staff to districts most impacted by emergencies. These teams have existed only since late 2002-early 2003 and their roles are still evolving, but they have played major roles in regional planning and response to emergencies, including outbreak situations.

XVIII. Recovery

Do the Commonwealth and its regions and localities have the capability to make a timely recovery from homeland security incidents and natural disasters?

Sub-Elements:

- Are recovery plans sufficiently flexible to take into account the full range of threats and consequences?
- Do recovery plans establish priorities for the recovery effort and address the costs associated with recovery and the time frame for restoration of services, facilities, programs, and infrastructure?
- To what extent can the private sector and volunteer groups participate in recovery activities pursuant to an emergency situation?

Comment: Through recent disasters (including hurricanes Floyd and Isabel), Virginia has incorporated continuous improvement mechanisms into this process.

XIX. Training & Exercises

Training. Do the Commonwealth and its local governments regularly assess their training needs, and develop and implement a training/educational program for public/private officials and emergency response personnel?

Sub-Elements:

- Has the entity performed an assessment of training needs and developed and implemented a training/educational program to support the program?
    - Does the training and education program comply with all applicable regulatory requirements?
    - Is the training of emergency management personnel and key public officials given high priority?
- Does the training contribute to awareness and enhance the skills required to develop, implement, maintain, and execute the program?
    - Do emergency personnel receive and maintain training consistent with their current and potential responsibilities? (This includes, for example, attendance at training events, conferences, workshops, exercises, seminars, and courses—including formal education and degree programs where practical and feasible.)
    - Is specialized training sought in areas related to threats confronting the jurisdiction?
    - Is awareness training and education of key officials provided?

- Is the frequency and scope of the training identified in the program?
    - Is training regularly scheduled and conducted in conjunction with the overall goals and objectives of the training program?
    - Is the scope of training consistent with the training needs assessment?
    - Is the training related to correcting action program deficiencies where possible?
- Are personnel trained on the entity's incident management system?
    - Do all emergency personnel undergo training on the incident management system of the program, including awareness of the operating systems of Federal, State and local governments, and first responder and volunteer organizations?
- Are records maintained documenting training conducted?
    - Do the training program records include the names of those who have received training, the types of training planned and conducted, and qualifications of trainers?

Exercises. Does the Commonwealth have in place a robust exercise program for testing and evaluating its preparedness and the preparedness of its local governments?

Sub-Elements:

- Are the Commonwealth and its local governments periodically conducting the full range of exercises (discussion and operations-based) to test their preparedness?
    - How often have Commonwealth exercises been undertaken, and how many exercises have been completed at the local level per year (in absolute and percentage terms)?
- Are the exercises conducted in accordance with DHS Homeland Security Exercise and Evaluation Program (HSEEP) guidance and NFPA 1600 Standards § 5.13?
- Are the exercises multidisciplinary and multiagency?
- Do the exercises' scenarios reflect potential threats and vulnerabilities?
- Do the exercises range in scope and increase in complexity over time?
- Does the Commonwealth or local government have an effective process to evaluate the results of the exercises, including the identification of capability areas where: 1) existing strengths are validated; and 2) improvements warranted?
    - Does the political subdivision have an improvement plan by which lessons learned from an exercise are turned into concrete, measurable steps that result in improved response capabilities?

Comment: In concert with DHS's Emergency Management Institute (EMI) program of resident and nonresident training, the Virginia Department of Emergency Management (VDEM) coordinates a wide variety of training courses in five major programs: Emergency Management, Hazardous Materials, Radiological Emergency Response, Public Safety Response to Terrorism, and Search and Rescue. The efficient and effective training of first responders, State and local government officials, volunteer organizations, and the public and private sectors is key to the Commonwealth's ability to minimize the impact of disasters on its residents. Individual training provides the critical link that bonds policies and procedures, organizations, and equipment together to contribute to a "safe, secure, and prepared Virginia."

Exercises are a key element of capability and performance measures because they refine needed capabilities and determine future performance measures. How is information gained from exercises acted upon?

As a component of the Commonwealth's comprehensive exercise program (CEP), the evaluation and assessment of exercises to validate strengths and identify improvement opportunities for the key response nodes/elements are critical for the State to meet its preparedness goals. The measurement of performance against a comprehensive, objective and straightforward set of criteria will provide those participating in training events with the most accurate assessment of their performance. While it may take time for organizations and jurisdictions to fully develop and practice their capabilities, the experience and incorporation of the "best practices" learned from a cycle of exercise activity conducted regularly will contribute significantly to achieving their preparedness objectives.

XX. Transportation

Are the Commonwealth's airports, bus and train stations, ports, bridges, rail lines, roads and highways, and tunnels for carriage of persons and cargo ("transportation infrastructure" or "assets") sufficiently secure? Are there plans and procedures in place to deal with potential threats to such critical transport assets in the event of a homeland security emergency, man-made accident, or natural disaster?

Sub-Elements:

- Have all such transportation assets been inventoried by the appropriate governmental entity and reviewed as part of the risk assessment process set forth above?
- Have all such transportation assets, whether publicly or privately owned and whether open to public or private transport, been legally licensed or registered in accordance with Commonwealth laws and regulations?
- Have all privately owned aircraft and other vehicles and vessels utilized in Virginia been registered or licensed in the state in accordance with Commonwealth laws and regulations?
- Have all such transportation assets developed, implemented, and funded preparedness plans that include elements on: physical and perimeter security; screening of passengers and luggage as appropriate; information security; coordination with local government and Commonwealth governmental authorities on issues that arise; and response to and recovery from man-made and natural disasters?
- Has the Commonwealth conducted or planned to conduct a study to systemically understand and address the interdependencies of transportation infrastructures with other infrastructures and systems of the Commonwealth, with respect to homeland security?

- Have the complementary roles of the responsible transportation agencies, including the Virginia Department of Transportation ("VDOT"), the Virginia Department of Rail and Port Transportation ("VDRPT"), the Virginia Port Authority ("VPA"), the Department of Aviation ("DOAV"), and the Department of Motor Vehicles ("DMV"), been adequately defined?
- Have the transportation providers in the private sector (e.g., Virginia Railway Express, airport commissions) been involved adequately in planning for Commonwealth preparedness?
- Have Commonwealth travelers, including private citizens and commercial vehicle operators, been adequately prepared to help prevent, respond to, and recover from man-made and natural hazards to the transportation infrastructure?
- Have priorities for investments in transportation security been developed systematically and designed for maximum efficacy for the level of investment?

Comment: Developing and maintaining transportation security is a difficult but important priority over the long-term. While some of the effort involves establishing appropriate procedures, other elements must rely on new and emerging technology that enables the detection of threats to transportation assets. New sensors and systems are under development and should be inserted into existing systems as expeditiously as possible.

In various transportation areas, the Commonwealth has developed and implemented plans. For example, the Virginia Area Maritime Security Committee ("AMSC") Circular No. 05-04 promulgates the Virginia Area Maritime Security Plan. The Maritime Transportation Security Act designated the Captain of the Port ("COTP") as the Federal Maritime Security Coordinator ("FMSC"). There are separate AMSC's for the National Capitol Region and Hampton Roads. Each respective FMSC has developed an Area Maritime Security ("AMS") Plan covering areas of responsibility. The plans take a port-wide command and control approach to deterring and responding to Transportation Security incidents ("TSI"). Plans are developed in consultation with the AMSC and key maritime stakeholders. As the national and regional guidance for many of the complicated issues touched by the plans continue to be refined, changes and lessons learned will be incorporated.

Conclusion

In sum, the performance measures set forth above are a beginning, and not an end point. These measures – generally in question form – are designed to ascertain what plans, procedures, and, more fundamentally, core capabilities have been put in place. They should be vetted by expert groups and other stakeholders, fleshed out in more detail, and supplemented with additional numeric or specific standards where possible and appropriate. As noted earlier in the report, as time goes by and capabilities are put in place, the measures should focus less on the "existence" of capabilities and more on their effectiveness.

The utility of the performance measures or standards delineated herein will, of course, ultimately be found in terms of their incorporation into a performance measurement program implemented by the Commonwealth. The task force therefore recommends that such a performance measure program be initiated, possibly under the auspices of the OCP with assistance from the Panel. The result should be a Performance Measurement Program that draws upon the measures set forth herein and builds in additional objective measures where possible. Understanding the scope and potential complexity of such a program, the task force recommends that the program initially adopt a "crawl before you walk" approach, maximizing leverage on ongoing activities (e.g., exercise and training programs), and consider the possibility of selected "pilot" efforts. These "pilots" would be designed to both prototype the measurement process and make early progress in high priority domains (e.g., interagency interactions in the National Capital Region).

Further, the task force submits the following recommendations for consideration by the Commonwealth in developing a Performance Measurement Program for its preparedness:

1. Assessment Time Frames, Methods, & After-Action Reports. Performance standards should not be simply a set of guidelines that collect dust on shelves. Hence, to ensure the standards are operational, the Commonwealth should establish a set of requirements for:

    - annual or biannual reviews of the Commonwealth and its local governments;
    - the use of a range of assessment methods, including periodic self-assessments, peer reviews (by other Virginia governments or other state governments), and assessments by the Commonwealth of local governments; and
    - a clear approach to establishing "after-action" reports in response to events and exercises with regard to performance measure assessments conducted, including a clear ranking or grading criteria (whether color coding or otherwise) that shows how well the government unit performed, an analysis of why the performance measures were not met (i.e., what barriers exist) and a process for follow up on recommendations to determine whether needed actions have or have not been taken.

2. Linking Performance Measures to Funding. It is our recommendation that the performance of local governments be taken into account by the Commonwealth as a significant factor in allocating or distributing Federal grants and other available state funds. Local governments are thereby put on notice of the prospect that their performance, including their management of grant funds (see Performance Measure V,

"Grant Functions," above) will in the future be considered along with other relevant funding factors in grant and other funding allocations or appropriations made by the Commonwealth.

3. Minimum Performance Measures. At the "enterprise level," as the performance measures set forth herein are further refined and made more specific, it is our recommendation that consideration be given, in some areas, to establishing some "minimum" performance thresholds that must be met by various levels of government.

Appendix I-5

Public/Private Cooperation Task Force of the Secure Commonwealth Panel

Recommendations to The Secure Commonwealth Panel And The Office of the Governor – Commonwealth Preparedness

May 10, 2005

Table of Contents

Members

Kay Goss, Chair
Senior Advisor for Homeland Security
Business Continuity and Emergency Management Services
Electronic Data Systems Corp. (EDS)

The Honorable Eugene J. Huang
Secretary of Technology

Robert P. Crouch, Jr.
Chief Deputy Secretary of Public Safety,

Steven M. Mondul
State Director, Security & Emergency Management
Department of Transportation

Tom Hassler
President, Virginia Emergency Management Association
Jefferson Lab

Michael M. Cline
State Coordinator, Virginia Department of Emergency Management

Frances L. Kernodle
President, Kernodle and Associates

Anne F. Thomson Reed
President, Acquisition Solutions, Inc.

Larry Smith
Emergency Services Director
Tappahanock, VA

Thomas C. Franklin, Ph.D
President/CEO, Universal Security Technology Group

William L. Radcliff
Homeland Security Advisor for SAIC

Debra Yamanaka
Homeland Security Advisor for SRA

Mark Penn
Emergency Management Coordinator
City of Alexandria

Archibald C. Reid
Federal Emergency Management Association, Retired

Introduction

Mission of the Task Force

Address issues regarding public/private partnerships for securing the Commonwealth's critical infrastructure.

Policy Issues

- *Determine how the Commonwealth, the Department of Homeland Security (DHS) and other Federal agencies can improve their working relationship in the area of critical infrastructure protection*
- *Improve communication between the public and private sectors on security and preparedness issues*
- *Improve public/private coordination on critical infrastructure emergency planning and exercises*
- *Ensure the business community, as a whole, is prepared for disasters*

Guiding Principles

When discussions of homeland security turn to the role, possibilities, and challenges of the private sector, they typically focus on four major areas:

Challenge 1: Security Screening

> *For example, some private sector leaders helped defeat a legislative provision by Congressman David Obey that would have mandated 100% screening on all cargo in the belly of a commercial airplane. They contended that this would be difficult, if not impossible, in the short term without putting some major bottlenecks into the global supply chain.*
>
> *Yet they know that we should be pushing for new tools and technologies to enhance cargo screening. The private sector's approach is that we should not impose new cost burdens on industry, which already pays billions of dollars in security user fees—16 billion dollars at seaports alone.*
>
> *The private sector advocates that we adopt a well-thought-out and strategic view toward securing our supply chain. We should spend time and money investigating new technologies and assess what economic benefit they would provide in addition to any promised security improvement.*

Challenge 2: SAFETY Act

The private sector believes generally that it is essential for DHS to fully implement the SAFETY Act. The Act provides liability protections for private sector firms to deploy technologies that might otherwise not be broadly available, so that private sector innovators would have an incentive to take risks and put new anti-terrorism technology in the field quickly. DHS has been slow to certify technologies and services for the SAFETY Act, but recently we have seen some improvement.

The private sector would like DHS to link specific procurements to SAFETY Act designation. We know that some parts of DHS, including the Transportation Security Administration (TSA), are fighting to link some of their upcoming requests for proposals to the Act—and a final decision has not yet been made.

Challenge 3: Information Sharing

There is a widespread perception in the public and private sectors that Federal authorities have much more information on threats and vulnerabilities than is being shared, and that we would all benefit if it were in fact shared.

Some industries are making great headway in this regard. In the transportation world, the Highway Watch program is a good example of creative thinking to address this challenge. It is one of several initiatives in information sharing that has resulted from the sector-specific Information Sharing and Analysis Centers (ISAC) model that is now operational as part of our Nation's critical infrastructure protection effort.

The public and private sectors agree that the State, Federal and local governments should increase the sharing of information with the private sectors.

While it is easy to say information sharing is a good idea, current events have demonstrated that implementation, even within the Federal government alone, is a challenge. Collaboration between governments at all levels and with the private sector will take years. It will require cultural change within our intelligence community and will by necessity be a system built on trust, which takes time to develop. But we all must work to promote an enhanced dialogue between governments at all levels and the private sector.

A critical part of this promotion is the necessary first step—setting up the legal framework that protects companies when they share information with the government. DHS has issued an interim rule to protect this information when it is voluntarily submitted to them, and we are hopeful that we will soon see a good final regulation that sets the foundation for robust information sharing.

As a complement to this first step, DHS is, we understand, drafting its thoughts on information requirements—that is, what information the government would like from the private sector. We hear repeatedly from those in government that our member companies *have information that would be useful if only they would share it. From our perspective, we would like to get beyond this rhetoric to a little more detail so that we can find a path forward in this critical area.*

Additionally, the private sector is beginning to advocate a government-wide re-assessment of how information is classified, and for what purpose. Far too often, we hear that information cannot be shared with private entities because it is classified. From our perspective, we are in a new era where robust sharing of intelligence information must be the norm, not the exception. The private sector feels an obligation to help the government modernize its intelligence capacity and shift the mindset from one of keeping all information close to sharing it more broadly, as appropriate.

By taking all these steps—setting the legal framework for information sharing, establishing information requirements, and reassessing how information is classified with the goal of classifying less and sharing more—the private sector will be better able to meet the threat of terrorism in partnership with the government.

Challenge 4: Cyber Security

The private sector is committed to increasing the awareness of cyber security throughout the business community and explaining cyber security in terms that all businesses understand.

While advances in information technology have brought tremendous productivity gains for businesses and information resources for everyone, these advances come with risks. The software that makes this information revolution possible operates based on a series of codes. An error in code affects the ability of the Internet in general, and your computer specifically, to operate. Humans create this code, and all humans make mistakes.

On a larger scale, entire segments of the U.S. economy are dependent on the Internet. As a result, there are those who are constantly looking for ways to launch an attack that could cripple the economy by bringing the Internet to a halt. For example, much of our power grid and financial services depend on the Internet for daily business operations. Internet dependent technology also is used to track packages, operate trains and control dams. Therein lies the daunting challenge. Our economy is propelled by complex, imperfect technology. The average user of that technology does not understand the threat, let alone how to protect against that threat.

For cyber security, unlike most of the other areas being discussed, there is no relatively simple regulatory or legislative solution. Technology simply advances too quickly. Instead, ultimately the market is better able to respond to cyber security challenges since market forces propel companies to be flexible, innovative and customer oriented. Regulations, in contrast, are reactive and constrictive.

The private sector counts on the market, believing it remains a powerful vehicle for increasing cyber security. Before this power is fully realized, however, we need to better *inform consumers on why cyber security is an issue that matters to them. They will demand more secure products, and successful firms will deliver those products.*

One step in this process is the development of a cyber security guide for small businesses. Created in conjunction with the Internet Security Alliance and others, this guide outlines 12 cost effective steps that resource limited small businesses can take to better secure their networks. For those of you who are interested in downloading a copy of the guide, you can do so from the US Chamber of Commerce Web-site http://www.uschamber.com/default.

Raising awareness is not the only solution to enhancing cyber security. Enhancing cyber security also requires the combined efforts of users, systems engineers, technologists, and senior executives: those who use software and hardware, those who make software and hardware, and those who manage enterprises that rely on software and hardware to make the company operate. While technologists have a responsibility to make secure products, end users have a responsibility to use those products securely. Cyber security is everyone's problem, and everyone can contribute to the solution.

Finally, the challenges facing our Nation and our Commonwealth are daunting; but they are not insurmountable. We can enhance our Nation's homeland security while also continuing to have a global supply chain that moves goods effectively, efficiently, and with the speed we are used to. It will take hard work. It will take patience. And it will take a commitment by both the public and private sectors to make policy choices as partners who need one another to succeed.

The Commonwealth's Task Force on Public/Private Cooperation in Homeland Security has attempted to develop some ways in which we can take our homeland security preparedness to a new and higher level, establishing a national model for other States in close public/private cooperation. These recommendations are discussed below.

Recommendations

I. Policy

Communications

The public and private sectors must increase their willingness and ability to share information, as this is vital to ensuring the cooperation needed to protect Virginia's critical infrastructure.

Issue 1 - Increase private sector awareness and access to government information.

Recommendations

1. The public and private sectors should work together to establish a protocol for information sharing to protect private industry data.

2. There is state and Federal law dealing with the non-Freedom of Information Act (FOIA) status of Critical Infrastructure Information (CII). Part of the problem is that industry does not trust the government's ability to withstand legal attacks on this statute. Thus, government must work with business to build up the trust necessary for information sharing.

Business Preparedness

The private sector owns and operates 80-90% of critical infrastructure. Thus, it is imperative that businesses be prepared for any risk and that the Commonwealth work with Virginia's businesses to assist their efforts.

Issue 1 - Businesses should develop emergency plans for any disaster, both man-made and natural.

Recommendations

1. Business should be prepared for disasters ranging from terrorist attacks to natural disasters to IT failures.

2. The Commonwealth's emergency plans should recognize that, while law enforcement is a key aspect of preparedness and security, it is vital to include members of the private sector, health experts, and representatives from other areas in the planning process, thus ensuring a comprehensive approach to preparedness.

3. One or more members of this task force should work to develop a template for the private sector (with special consideration of small business) that would feature "Five Easy Steps to Emergency Preparedness." The template could be refined by the full task force and submitted to the State for publication on its website. The Commonwealth could print this plan cost-efficiently and distribute it statewide through community offices of emergency preparedness or through local Chambers of Commerce.

   Also, "Five Easy Steps to Emergency Preparedness" could be one of the information sheets inserted in packages for new business owners in Virginia communities and distributed by the Commonwealth when companies certify in any of the special initiatives, including certifications through the Department of Minority Business Enterprise and the Virginia Department of Business Assistance.

   In addition, this information sheet could be a part of any package that is prepared for seminars or workshops that may evolve as a result of these recommendations. Incidentally, the task force recommends that using the term "emergency preparedness" rather than "security" as the word "security" is too widely used.

Defining the Threat

The public and private sectors need to know what threats Virginia's critical infrastructure faces.

Issue 1 - To best prepare for threats, there should be agreement between the public and private sectors on which areas of critical infrastructure need the most improvement in emergency preparedness.

Recommendations

1. The public and private sector should work to develop a common list of threats to Virginia's critical infrastructure, as well as which infrastructures require additional emergency preparation.

2. Both sectors also need to develop a common definition of "threat" and of what level of preparedness is satisfactory to meet the threats faced by critical infrastructure in Virginia.

3. Both sectors should determine when public resources will be used to protect private assets during times of high alert.

Disaster Response Coordination

The public and private sectors need to have a coordinated response plan for disasters, thus ensuring the most efficient response and recovery possible.

Issue 1 - How do we successfully leverage the multitude of skilled volunteers from the private sector to respond to a disaster?

Recommendations

1. The public and private sectors should develop mutual aid agreements and Memoranda of Understanding (MOU) for emergency volunteers.

2. The Virginia Department of Emergency Management should research this issue and work with a secretariat to develop legislation that would protect against lawsuits.

II. Process

Communications

The public and private sectors need to set up a communication process.

Issue 1 - Who will be the key players in communications between the public and private sectors?

Recommendations

1. Local government inspectors can serve as educators to local business because they already have a relationship and can provide information and assist in the business preparedness and security measures during annual visits.

2. The government can use local Chambers of Commerce, Rotary Clubs, and other local business organizations to market preparedness and security information as well as to disseminate information to smaller businesses during an emergency.

3. Governments can work with local business organizations to hold joint public/private conferences on preparedness and security.

4. The local emergency manager should serve as the “go to” person and coordinator during a disaster.

Issue 2 – Improve the working relationship between the Commonwealth and DHS in the area of critical infrastructure.

Recommendation

The Commonwealth should develop a stronger dedicated coordination structure to ensure coordination with DHS.

Identify Vulnerabilities

The public and private sectors need to work together to assess threat and prepare for emergency response.

Issue 1 - Ensure the business community, as a whole, is prepared for disasters.

Recommendations

1. The Commonwealth should conduct preparedness assessments of local businesses and put a sticker in the window of the businesses that pass or meet a certain standard. DHS funding for this program would be helpful.
2. The Office of Commonwealth Preparedness (via the Virginia Department of Transportation) is doing risk assessment on those facilities identified on the DHS Critical Infrastructure list as well as some others. This list is under revision. Private industry can use public domain guides to complete risk assessments as well. The Commonwealth should encourage this practice in the business community—perhaps through the private security industry.

3. The Commonwealth should leverage risk assessments, studies, and surveys etc., already completed by other entities, and determine how it will share that information.

4. Governments should involve local businesses in tabletop exercises.

III. Implementation

Communication Framework

The public and private sectors need to designate how they will communicate on a regular basis and during emergency situations.

Issue 1 - The government needs to disseminate information to the business community effectively and efficiently.

Recommendations

1. Text messaging is an effective method for informing private building security personnel during an incident. Building security is a valuable resource and can better coordinate efforts with local law enforcement when responding to a disaster if kept up-to-speed on response actions.

2. The Commonwealth must be prepared to consistently update information so the private sector can rely on it at any time, via both a website and radio. * The Commonwealth could sponsor a program, such as the one in Chesterfield, to give free weather radios to businesses that cannot afford one.

3. The National Incident Management System (NIMS) is an established framework by which the private sector could communicate with law enforcement.

4. The Virginia Information Security Exchange (VISE) can be used to bring the key government and private sector preparedness and security officials together to communicate.

5. The Fusion Center will foster the convergence of the cyber and physical ambit (enabler to monitor, manage, control and report on the connected elements within the entire system all within a single, integrated, common operating environment).

6. Government can partner with the media to disseminate information to the business community.

Issue 2 - What are the telecommunications requirements to ensure the continuous, uninterrupted flow of information, during a disaster?

Recommendations

1. Consider VoIP—Voice over IP—a major step in the evolution of rich multimedia communications for businesses and consumers that are more personal, better integrated, and deliver better value to communications.

2. The local, State, and Federal governments should cooperate to ensure first responders are able to communicate during a disaster. The government could work with the phone companies to have a line set aside for the first responders to use during a disaster.

Emergency Preparedness Information

To ensure the protection of critical infrastructure, businesses will need resources that provide the information they require to best prepare for disasters.

Issue 1 - Ensure the business community has the information and expertise it needs to best prepare for disasters.

Recommendations

1. Companies that have established plans and are prepared could serve as mentors to other businesses to teach them how to best prepare for a disaster. The Commonwealth should encourage mentor protégé programs.

2. The State could host a best-practices website that would better educate businesses, particularly smaller businesses with limited resources, on how to best prepare for and recover from a disaster.

Conclusion

Nearly four years after the devastating attacks of 9/11, homeland security remains a top priority for national, state, and local leaders in the public and privates sectors throughout the Nation. However, despite this heightened focus on our Nation's and our Commonwealth's critical vulnerabilities, it is apparent that much more can and should be done to guarantee the protection of our citizens. Homeland security is a process, not a one-time event.

Our Commonwealth's business leaders must be better prepared to respond to the threat to our security and should have a basic plan of action to inform and protect their employees and the citizens of their communities, as well as their facilities. Communication from government organizations and public safety agencies to businesses, media, nonprofit organizations, volunteers and citizens should be clear and actionable.

Business leaders should be open to cooperation and collaboration at the Commonwealth and community levels, working to build strong public private partnerships that offer both government and business leaders the information, tools, and resources they need to meet their mutual interest in protecting the Nation's vital infrastructure.

With 85% of the Nation's critical infrastructure in the hands of the private sector, industry has an important role to play in the current environment. Accordingly, businesses have an opportunity to build stronger bonds with government and work together as partners in preparedness.

Appendix J

Secure Commonwealth Initiative Strategic Plan Proceedings of Public Hearings

Office of the Governor
Secure Commonwealth Panel
Commonwealth of Virginia

October 2005

INTRODUCTION

Immediately after the attacks of 2001, then Governor James S. Gilmore, III initiated a rapid 68-day review of Virginia's readiness to address terrorist threats. This effort, referred to as the Virginia Preparedness and Security Panel, engaged local, state, federal and private sector leaders in assessing Virginia's overall readiness. Following his election in November 2001, Governor-elect Mark Warner established Virginia's first Cabinet rank position to synchronize the full range of statewide preparedness initiatives.

The establishment of the Secure Virginia Initiative, subsequently re-designated the Secure Commonwealth Initiative, shortly followed these initial actions. This Initiative was designed to carry forward the review begun in the prior administration, and has continued for four years. Arguably these steps, combined with the Commonwealth's history of preparing, preventing and responding to emergencies and disasters, to include terrorist threats, have provided an invaluable foundation that has allowed Virginia's preparedness efforts to progress.

The strategies and initiatives outlined in the strategic plan will enable the Commonwealth to realize the goal of a more safe and secure state. After four years of review, analysis, debate and decision-making, Virginia has produced a plan to continue progress on its preparedness, prevention, response and recovery capabilities.

In order to assure that the Secure Commonwealth Panel has addressed the key long-term goal of protecting the Commonwealth and its citizens, a series of public hearings were held between September 14 and September 28, 2005 to receive comments on the plan. Twelve public hearings (at 1:00 PM and 6:30 PM each day) were held in six venues across the Commonwealth. These were:

September 14, 2005	Region 7	Annandale, VA
September 20, 2005	Region 4/6	Christiansburg, VA
September 21, 2005	Region 3	Lynchburg, VA
September 22, 2005	Region 2	Culpeper, VA
September 27, 2005	Region 5	Hampton, VA
September 28, 2005	Region 1	Chester, VA

At each hearing, a presentation was given to provide the participants with an overview of the plan. Over 90 people representing private citizens, first responders, emergency management, public works, health, agriculture, private industry and utilities attended the hearings. Their comments, questions and concerns are outlined in this document. All comments brought a unique and enlightening perspective to the discussion on the strategic plan.

About This Document

This document contains a general summation of the comments of the participants. It is not an exhaustive transcript of the proceedings. The contents are organized by hearing date. Each hearing summary includes at its beginning "Key Strategic Issues" that represent a broad, general topical area of particular interest for review by the Secure Commonwealth Panel. The document also includes introductory and closing remarks by the hearing chair and participating members of the Secure Commonwealth Panel.

Table of Contents

SUMMARY OF KEY STRATEGIC ISSUES

1. Communications

- Communicating with government workers and the general public
- Improve risk communications and getting the message out in specific ethnic communities
- Improve regional public information and communicating with a mobile population
- Need to articulate risk management methodolgies to the business community
- Fully examine the strategic issues associated with communication; how do we communicate, what do we communicate, and how do we not leave anyone out, in particular, special needs populations
- Address the key areas of communications and public education
- Improving our capability to communicate with the public is a key strategy. This includes education and dissemination of "protective measures" (evacuation, shelter-in-place. etc.)
- Prevention strategies need to be addressed as part of public education
- Specific issues related to special needs populations and general education of the public on readiness and preparedness
- Public involvement in the preparedness planning and exercise process
- Prevention should be a primary focus of the strategic plan (gangs, fire, nuclear, natural hazards, etc)
- Use of other technologies to enhance communications during an emergency

2. Regions

- Regional strategic plan coordination
- Response is regional, so planning should be regional as well
- Smaller/rural communities need to change the "it won't happen here" thought pattern. If they aren't a primary target, they may be involved in the regional/national response
- Regional planning extends beyond state lines
- The entire concept of regions working together and responding in support of each other

3. Resource Management

- Key objective that "risk" drives funding as opposed to population density
- Local connections between responders need to be maintained regardless of funding streams and priorities associated with those funds
- Rules and regulations are vital and necessary, but should not stand in the way of getting needed resources and doing what's necessary to save lives
- Resources to implement strategies will be limited. Performance measures are the key to funding and implementation

4. Mass Casualty and Fatality Management

- Examination of issues regarding handling of mass fatalities and staffing
- Family assistance and reunification are vital services that need to be addressed
- Mass fatalities need to be addressed in the strategic plan

5. General

- Challenges with standardization of training
- Specific issues for each area of the agricultural industry need to be addressed within the respective group
- The need for a full-time emergency manager must be articulated to sustain local buy-in.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Annandale Fire Station #8, Annandale, VA
September 14, 2005
Region 7

KEY STRATEGIC ISSUES

- **Specific issues related to special needs populations and general education of the public on readiness and preparedness**
- **Challenges with standardization of training**
- **Regional strategic plan coordination**
- **Communicating with government workers and the general public**

Hearing Called to Order: 1320

The meeting was called to order by George Foresman, Director of the Office of Commonwealth Preparedness and Chairman of the Secure Commonwealth Panel (SCP). Mr. Foresman introduced other members of the Secure Commonwealth Panel in attendance: Senator Janet Howell, John Quilty, and Chief Michael Neuhard.

George Foresman:

- Description of the process for completing the strategic plan and a description of the Secure Commonwealth Panel and it's role.
- The Panel is comprised of diverse experts who bring many different viewpoints to the table, from local government officials, to state cabinet officials, to federal government employees to private sector representatives. State agencies have also played a key role in the plan's development to develop an enterprise-wide approach statewide as well as spanning various levels and sectors of state, local and federal governments.
- Explanation that the plan was compiled from sub-panel input as well as the Panel's vision for the future of Virginia regarding preparedness
- The plan is meant to be a starting point for the next administration to maintain momentum in the area of preparedness and it will take years and multiple administrations to realize all of the "end goals" laid out in the Plan. The Plan is also looking at preparedness from a 50,000 ft. level to set the groundwork for other plans.
- The Public Hearings are designed to include citizens in the process, as citizens are a key component in maintaining a safe, secure and prepared Commonwealth.

Members of the SCP made additional opening remarks.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

Additional panel member comments. Chief Neuhard recommended that the public recognize that Appendix J has a matrix which aligns the Strategic Plan with national priorities and goals.

PUBLIC COMMENT PERIOD

Mark Penn (Alexandria Emergency Management):

- Commented that the Secure Commonwealth Initiative Strategic (SCIS) Plan provides a great framework and is an excellent plan. He would like to see the implementation level and appendices. No issues or clarifying questions at this time.

David Schwengel (Northern Virginia Regional Commission):

- Asked where the plan was in relation to other plans in the US?
- *Chairman Foresman:* Much discussion in other states focuses on operational and implementation plans, not on a comprehensive strategic approach to preparedness.
- *Chief Neuhard*: Responded that the SCIS Plan is an overarching plan that is conceptual. The SCIS Plan will serve to help local governments in their preparedness activities. Chief Neuhard added that Appendix J of the SCIS Plan aligns the document with national strategies.
- *John Quilty*: Offered that the plan takes advantage of work in other states by providing a systematic review of performance measures taking lessons from other states. See the Performance Measures Task Force report in Appendix I.
- *Senator Howell*: Commented that so far, all recommendations for legislation from the panel have been implemented, with one exception. And this document is important for legislators because many do not have the background and experience to produce something like this themselves. Thus, this plan gives legislators a blueprint for next steps.
- *Chief Neuhard*: Offered that only a small percentage of the panel is present, the panel is quite large and has broad representation.
- *Senator Howell*: Commented that interoperability is also a major focus for the strategic plan.

Cindy Jones (Alexandria MRC):

- Ms. Jones felt there was not sufficient emphasis on people. She asked "where is the education of people, the inclusion of multi-lingual and special populations, citizen preparedness and how do you communicate with those populations?"
- *Chairman Foresman*: Mr. Foresman acknowledged the need to bring out the human-to-human focus and to get information out to the masses.
- *Chief Neuhard*: Offered the observation that the Citizen and Community sub-panel of the Secure Commonwealth Panel expressed deep concern about the issue of community involvement and attempted to insure that community support was an imbedded within the panel's initiatives.
- *Senator Howell*: Commented that people don't always do what the government plans for them to do. Senator Howell expressed a desire that the plan attempt to bring that reality into the SCIS plan.

Chairman Foresman question directed to Anwar Othman (VDOT):

- "Do you feel that you have the information necessary to coordinate with local partners on a lot of transportation planning initiatives as a **government worker**?"
- Response from Mr. Othman: Yes, through constant email communication.

Donald Amos (Herndon Police):

- Remarked that he was glad to see that smaller jurisdictions are included in the SCIS plan.

Melvin Byrne (Dept. of Fire Programs):

- Expressed that he likes what he sees, but has concerns about standardized training. He acknowledged that there will be challenges with EMS standards.

- *Chairman Foresman*: Remarked that he appreciated the comment. We are allocating funds to communities and we must develop performance measures to justify funding and measure achievement to the goals.
- *Chief Neuhard:* We have tried to address these issues through the state fire associations for inclusion. Our approach is the use of standards as opposed to mandates.

Leon Buckley (City of Manassas):

- Mentioned that he was pleased to see improvements being sought in emergency medical services funding and in disaster staffing.

Cindy Causey (VDEM):

- Commented that "This is a great start but State employees at the regional level are not in tune with overall strategic level. We need to get the regional groups to work with the locals. They are not getting the message within the state agencies."
- *Chairman Foresman*: Responded that the Panel needs to be more definitive in the strategy regarding the regional focus.
- *Chief Neuhard*: Asked Ms. Causey if there were a strategy that she could describe to make that work?
- *Ms. Causey*: Responded that regional teams were put together to get this process started. But there is not wide understanding in state government that local government was part of this process and they all need to be involved. The State needs to work on flow of information in order to initiate work with locals.
- *Chief Neuhard*: "The challenge is that the state agency regions not aligned."

Dave Schwengel:

- Mr Schwengel mentioned that he felt the Panel needed to address the ability to communicate with the public and within regions. He felt there are 3 key participants,
    1) General public
    2) Government employees
    3) Volunteers
- *Anwar Orthman*: Concurred with the communications issues between the state and locals must be improved.
- *Chairman Foresman*: Stated that communication is an important subject area as well as mutual-aid assistance and support in the Commonwealth. Mr. Foresmen queried the Panel whether they had an adequate strategy in place that addresses governmental workers communications and response.

Secure Commonwealth Panel Final Comments.

Sen. Howe: "Thank you. We want and need this input."

Chief Neuhard: "Thanks for being here. I am positive that we have some things to go back and look at"

John Quilty: Stated that regionalism needed to be more effectively addressed in the plan.

Chairman Foresman: Offered that the public who wished additional information could visit the web site for the Office of Commonwealth Preparedness at http://www.commonwealthpreparedness.virginia.gov. Those wishing to add comments or ask questions could email the Office of Commonwealth Preparedness until 8pm on September 28th at: ocp@governor.virginia.gov.

Public Comment Period Recessed: 1515

Public Comment Period Called to Order: 1645

Public Comment Period Adjourned: 1647

Secure Commonwealth Initiative Strategic Plan Public Hearing
Annandale Fire Station #8 - Annandale, VA
September 14, 2004
Region 7

KEY STRATEGIC ISSUES

- **Improve risk communications and getting the message out in specific ethnic communities**
- **Improve regional public information and communicating with a mobile population**

Hearing Called to Order: 1843

The public hearing was called to order by George Foresman, Director of the Office of Commonwealth Preparedness and Chairman of the Secure Commonwealth Panel. Chairman Foresman introduced The Hon. Jane Woods, Secretary of Health and Human Resources, and The Hon. Kate Hanley, members of the Secure Commonwealth Panel.

George Foresman:

- Description of the process for completing the strategic plan and a description of the Secure Commonwealth Panel and it's role.
- The Panel is comprised of diverse experts who bring many different viewpoints to the table, from local government officials, to state cabinet officials, to federal government employees to private sector representatives. State agencies have also played a key role in the Plan's development to develop an enterprise-wide approach statewide as well as spanning various levels and sectors of state, local and federal governments.
- Explanation that the plan was compiled from sub-panel input as well as the Panel's vision for the future of Virginia regarding preparedness
- The plan is meant to be a starting point for the next administration to maintain momentum in the area of preparedness and it will take years and multiple administrations to realize all of the "end goals" laid out in the Plan. The Plan is also looking at preparedness from a 50,000 ft. level to set the groundwork for other plans.
- The Public Hearings are designed to include citizens in the process, as citizens are a key component in maintaining a safe, secure and prepared Commonwealth.

Sec. Woods offered opening remarks.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

Chairman Foresman then framed the discussion on the strategic plan.

PUBLIC COMMENT PERIOD

Gloria Addo-Ayensu (Fairfax Public Health Director):

- Comment on the Health and Medical section, 2nd bullet under new initiatives. Recognize issue of ethnic diversity in northern VA and how they receive information within their communities.
- *Chairman Foresman:* Do we have enough emphasis on risk communication?

- *Kate Hanley*: Northern Virginia is spread out and there are many different media/communication contacts to get the word out to the various communities. The Secure Commonwealth Panel's task force on communication discovered that we rely on the private sector, so our communication is only as good as the private sector infrastructure.
- *Ms. Addo-Ayensu:* (references *Redefining Readiness: Terrorism Planning Through the Eyes of the Public*[1], a study on communicating with the public in an emergency) People don't trust the government, they trust their own resources.
- *Ms. Hanley:* Need to identify redundant communication techniques and how to get the message out to those special populations.
- *Ms. Addo-Ayensu*: Majority of information has to be disseminated pre-event, in order for people to gain understanding of the issues. Earn the respect of being a "trusted source".

Roy Shrout (Fairfax OEM):

- Related issue with the transient population, balancing those commuting in to and out of a locality. Fairfax dealing with large disabled population and trying to figure out how to work with them.
- *Chairman Foresman:* We encourage people to tune into their own "local" media to find out information, but if they are out of the area, will they get the "local" information?
- *Ms. Hanley:* Some communities don't have "local" media and the regional media doesn't address all localities. A lot goes on in jurisdictions that other first responders don't know about.
- *Chairman Foresman:* Ties back into earlier discussion on how to best communicate with federal, state and local governmental workers.
- *Sec Woods:* We have to establish some level of "dependency" to know the location of special needs populations in order to move them to areas of refuge in an emergency. What are the options to prepare with them? Need to build and practice from the citizen to the neighborhood to the community levels.
- *Ms. Addo-Ayensu:* Talking to the community helps determine best use of limited resources.
- *Chairman Foresman:* We need a specific focus in the strategy on special populations including non-English speaking population.
- *Sec. Woods:* There are special needs groups defined by time of day, i.e., latchkey kids.

Reuben Varghese (Arlington County Public Health Division):

- Risk communications critical with public education. During Katrina, so many voices talking, that people didn't know to turn. Should the media be responsible for accuracy in reporting factual information? Challenge to the overall document, that this is a strategy and that realization that implementation is difficult.
- Need to address animal health in document. People do not want to evacuate without their pets.
- *Chairman Foresman:* Media has a moral/ethical responsibility for getting and providing information. Need to have good connectivity to broadcast media. Whole success of plan is implementation. Moving from making recommendations to implementing them. A significant part of implementation is performance measures and that is tied to funding.
- *Ms. Hanley:* Media can be an ally in communicating preparedness and risk management information to the public.

Public Comment Period Ended: 1947

1.

A(v)[1] Lasker RD, *Redefining Readiness: Terrorism Planning Through the Eyes of the Public.* New York, NY: The New York Academy of Medicine, 2004.

Secure Commonwealth Panel Final Comments

Ms. Hanley: Need to do this again in Northern Virginia with more advanced notice and not at rush hour. Need more citizen input. There are citizen groups and Citizen Corps groups in NOVA that should be invited. Suggested multiple venues and local cable channel.

Chairman Foresman: Meeting closed at 2007.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Montgomery County Government Center - Christiansburg, Virginia
September 20, 2005
Regions 4 & 6

KEY STRATEGIC ISSUES

- **Specific issues for each area of the agricultural industry need to be addressed within the respective group**
- **Response is regional, so planning should be regional as well**

Hearing Called to Order: 1305

Robert Newman (Deputy Assistant to the Governor for Commonwealth Preparedness):

- Strategic plan has great merit, preparing VA for all types of emergencies.
- Transcend administrations and borders, should not be lost when new governor takes office.
- Developed as a five-year plan, new governor can capitalize if something happens.
- Public hearings are taking place to solicit comments and make changes before the ink dries.
- Plan is work in progress.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

PUBLIC COMMENT PERIOD

Larry Seamans (VA/MD Milk Cooperative):

- The cooperative covers 11 states.
- Bio-security issues regarding dairy farms is different from other farms.
- Need to develop practical, cost-effective standard operating procedures (SOPs).
- Labs for testing and standardizing interstate protocols.
- Submitted a tabletop exercise they went through with NC Dept of Agriculture to his written comments.
- Recommendations include moving animals 50 feet off the roads/farms 50 feet from roads; scheduled deliveries at farms to eliminate confusion; showering personnel and keeping the tankers off the farms. Everything possible to stop transmission of viruses.
- *Bob Newman:* Dr. Don Butts will receive this information at the VA Dept of Agriculture and interface with Mr. Seamans before the end of the week.

Richard (Rick) Burch (Fire Chief, Roanoke):

- Timetables regarding surveys, planning, etc. have all become very rushed which lend themselves to less-than-superior product.
- *Bob Newman:* More areas are becoming regional as opposed to national, because it's more efficient and more responsive, but all in all, the problem is known and improvement actions are being taken.

Hearing ended at 1445.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Montgomery County Government Center - Christiansburg, Virginia
September 20, 2005
Regions 4 & 6

KEY STRATEGIC ISSUES

- **Public involvement in the preparedness planning and exercise process**
- **Key objective that "risk" drives funding as opposed to population density**
- **Smaller/rural communities need to change the "it won't happen here" thought pattern. If they aren't a primary target, they may be involved in the regional/national response**

Hearing Called to Order: 1830

Robert Newman (Deputy Assistant to the Governor for Commonwealth Preparedness):

- Strategic plan has great merit, preparing VA for all types of emergencies.
- Transcend administrations and borders, should not be lost when new governor takes office.
- Developed as a five-year plan, new governor can capitalize if something happens.
- Public hearings are taking place to solicit comments and make changes before the ink dries.
- Plan is work in progress.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

PUBLIC COMMENT PERIOD

Neal Turner (Montgomery County Emergency Management):

- 50 security recommendations – came from sub-panels to panels and on to governor through Secure Commonwealth Initiative.
- There currently is nothing keeping that money from going up to Northern VA, however, it's all based upon how well the grants are written (i.e., Radford Munitions Plant). That's why things have gone regional – see AM minutes.
- There need to be mechanisms for drills and exercises done at the local level. That can't be put into the plan but rather on the operational level, since those people can put their hands on the plans and actually supply the funding (from their pot of money at state).
- The performance measures appendix focus on first responders and operational planning and their execution, plus their evaluations.

Mike Wilson (APCO):

- Involving everyone in NIMS because it's connected to money, but also because it's a unified command structure for everyone who may be involved or be there.
- If you're a responder, we want to train the people ("it's not going to happen to us"), and the money will come later.

Chad Weaver (VA Department of Aviation):

- Evidently, new intelligence continues to read that general aviation is a target, and the Montgomery County Executive Airport (LeerJets) will be contacted regarding further information about security, training, etc.

Hearing ended at 1945.

*This hearing was informal due to a smaller group of attendees.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Central Virginia Training Center - Lynchburg, Virginia
September 21, 2005
Region 3

KEY STRATEGIC ISSUES

- **Regional planning extends beyond state lines**
- **Local connections between responders need to be maintained regardless of funding streams and priorities associated with those funds**
- **The need for a full-time emergency manager must be articulated to sustain local buy-in.**

Hearing Called to Order: 1310

George Foresman:

- How do we manage/mitigate risk? Respond/recover? Without them, we can't survive in the long-term.
- It has to be sustainable and a transition across governments with measurable success over long-term.
- Recommend Office of Commonwealth Preparedness continues because much work has yet to be done– continuity is smarter and more effective.
- How do we make sure fire, police, health, etc. can deal with next disaster together? It's not if but when and how… and together.
- The citizens don't care how a response and recovery effort happens, but that it happens timely and effectively – not local or state or federal; just someone who can help.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

PUBLIC COMMENT PERIOD

Steve Eads (Emergency Management Coordinator with Henry County):

- Compliments on plan, easy to read.
- Good that it's an all-hazards focus and not just towards terrorism.
- 80% funding now is just terrorism, but emergency management runs the gambit from tornadoes to floods to hurricanes – emergency management is all-hazards. The formula for distribution from the federal government is trying to be more equitable.
- Northern Virginia, Richmond, Tidewater definitely have the most people, however, people do live west of Charlottesville, and there are targets out that way.
- Would like to see more representation from southwest Virginia on the Secure Commonwealth panels would be great.
- Communication since 9/11 has improved, however there's still room for more.
- Also, regionalization needs to extend beyond state lines – one border is NC, and they would like to do cross-border projects.
- *George Foresman:* Is everyone still getting what they need? We've got to address that one over and over, and we'll continue to do that. Also, the regional issues with NC.

Chris Stemp (Franklin County):

- EMS has been mentioned many times in the plan, and so frequently, EMS is pushed aside, so thank you for that.
- This plan calls for full-time emergency coordinators which is great, however a better look at how to fund those positions needs to be taken into consideration.
- The funding formula needs to allow for transient populations, like tourists.
- We depend on most of our Homeland Security funds to buy our basic equipment, and if we didn't have it, we couldn't afford most of our stuff.
- Also, constitutional (elected) positions vs. those who are qualified and have the skills.
- *George Foresman:* Elected folks do it because they feel as though they can do the best job possible. We also need to make sure that we give them the tools that they need to do their jobs. We need a summit of key officials in VA to support public safety over the long term.

Steve Eads:

- Full-time emergency manager (EM) concept that is addressed – but most EM's wear multiple hats. I am one of them and am pulled in different directions. What is your idea?
- *George Foresman:* 75% of the jurisdictions do it as a dual-responsibility. We need to get the 50 most populous cities in VA and get them to dedicate their EM as full-time as our first benchmark.

Jack Jones (Bedford Co.):

- Glad to be part of the audit, because we took a lot of time to show pictures and explaining reasons why they purchased something. Very useful for both sides.
- I'm also a full-time EM, but it needs to be encouraged and funding would certainly help.
- Credentialing would certainly help when it comes to set down qualifications for specific positions.
- *George Foresman:* Locals actually ended up educating the auditors on certain practices, because they knew just what they should be showing and what to look for. Next generation will be performance measures – benchmarks to judge where we're at and how we've done along the way.

Marvin Sheldon (Farmville, Southside Community Hospital):

- How does the community response work?
- It's important to the hospital, because we've shown up at things that were supposed to be TTX ?but turned out to be slide shows.
- *George Foresman:* We're instituting performance measures in the next 12 months. "No community left behind" as far as preparedness goes.

CLOSING STATEMENTS

George Foresman:

- Comments and questions will be accepted for the plan until the last public hearing is the 28th (Wednesday) at 8pm.

Hearing ended at 1420.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Central Virginia Training Center - Lynchburg, Virginia
September 21, 2005
Region 3

KEY STRATEGIC ISSUES

- ❖ **Need to articulate risk management methodologies to the business community**

Hearing Called to Order: 1835

George Foresman:

- How do we manage/mitigate risk? Respond/recover? Without them, we can't survive in the long-term.
- It has to be sustainable and a transition across governments with measurable success over long-term.
- Recommend Office of Commonwealth Preparedness continues because much work has yet to be done– continuity is smarter and more effective.
- How do we make sure fire, police, health, etc. can deal with next disaster together? It's not if but when and how… and together.
- The citizens don't care how a response and recovery effort happens, but that it happens timely and effectively – not local or state or federal; just someone who can help.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

PUBLIC COMMENT PERIOD

Lee Carr: (Bedford Chamber of Commerce):

- Discussion on improving communication about preparedness with smaller communities and businesses because there is a sense that terrorists will not attack them.
- Also need to better communicate with citizens on how to prepare for a disaster of any kind.
- State offices are not pushing information down to local offices on a continuous basis.

*This hearing was informal due to the lack of attendees (one of the two was an SME who had attended the two previous sessions in Christiansburg).

The Hearing ended at 1929.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Culpeper District Auditorium - Culpeper, Virginia
September 22, 2005
Region 2

KEY STRATEGIC ISSUES

- **Examination of issues regarding handling of mass fatalities and staffing**
- **Use of other technologies to enhance communications during an emergency**

Hearing Called to Order: 1305

Bob Newman:

- Secure Commonwealth Initiative began by Governor Warner after 9/11 for terrorism and natural disasters, envisioning cooperation with the Department of Homeland Security (DHS) and VA.
- Created Secure VA Panel (can only stay in effect for two years), which evolved into Secure Commonwealth Panel. The Office of Commonwealth Preparedness came out of that.
- Discussion stimulates conversation on issues for participation to help complete this plan – want to give to Governor Warner by mid-October. It's supposed to provide a roadmap for the next five years thus providing the next administration with "the road ahead".

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

PUBLIC COMMENT PERIOD

Joe Lenig (VA Broadband, LLC.):

- Building a network over VA, 17 counties, etc. and would like to incorporate this technology into preparedness program.
- *Bob Newman:* Resiliency and redundancy are key to interoperability of communications and capabilities; will pass this information along through our vendor process.

Nancy Bull (Medical Examiners Office):

- Need to notify office of the medical examiner in statewide drills and in disasters.
- We have a 24/7 phone line to monitor death reporting incidents throughout the state which may not be obvious at first which might be bioterrorism – the hospitals, state, police, etc. should use this to work out the bugs, but so far, less than optimal use is happening.
- Trying to recruit Medical Examiners (ME's). There has been no fee increase since 1980 (only $50, need to have the General Assembly pass a fee increase to recruit more medical examiners).
- *Bob Newman:* I met with Secretary Woods this morning and she wants to increase the fees with Homeland Security money. The hotline – the hospitals have a chat room which links all of them which is the hospital side of WebEOC.

Hearing ended at 1350.

*Two participants arrived late, 240p, asking if the hearing was over. Mr. Newman asked if they would like to sit and talk and they provided the suggestions below.

Informal hearing came to order at 1445.

Philip Myer (Fauquier):

- Background checks for all first responders are very important, including volunteers – EMS has that requirement. It would be nice, though, if there were a standard process with basic documents, standardized forms, etc. rather than just saying we should do it. Can the Attorney General's office facilitate this?
- Also, if you need money and we're going to give it to you, there should be a questionnaire that asks what you need and what you're looking for, and what you don't want to have it limited to – not just HAZMAT gear.
- Keep as many functions within VDEM as possible to eliminate more bureaucracy.
- Full-time Emergency Management Coordinator is another unfunded mandate… it's about time they finally get with it and have those positions at least.
- Need guidance for background check information.
- Can something be done to address problems first responders face when differing power companies cannot move downed power lines that are not their own to allow for search and recovery efforts?
- Funding forms, when a locality checks that it will not use a certain type of equipment it should not be permitted to buy this and should instead go toward a regional purchase.
- We'll start teaching all-hazards in school curricula, which is great but it should read more directly in the plan. Something called RiskWatch.
- Towns get some of county's homeland security grants and do not always use them in a timely manner, how can we work to fix this relationship, as not all towns and counties work well together?
- *Tim Lockett:* FEMA multi-hazards safety course covers all of that.
- *Philip Myer:* Also, like the fact that jurisdictions must turn in receipts before they get their money for their expenditures.
- *Bob Newman:* We (Mary Warder) a will look into the "$4-for-life" and "full funding from the fee" situation, because no one was able to explain those specific terms at the time. WebEOC is also useful and would be good for everyone to have access to.

Colleen Dawsen:

- Also, keeping some of your trainers in-state when deploying help a disaster, because you don't want to lose people who can train additional volunteers outside of the disasters.

Informal hearing ended at 1540.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Culpeper District Auditorium - Culpeper, Virginia
September 22, 2005
Region 2

The evening session (1830) was not called to order by the Chair due to no public being in attendance at the meeting.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Hampton Roads Convention Center - Hampton, VA
September 27, 2005
Region 5

KEY STRATEGIC ISSUES

- **Prevention should be a primary focus of the strategic plan (gangs, fire, nuclear, natural hazards, etc)**
- **The entire concept of regions working together and responding in support of each other**
- **Fully examine the strategic issues associated with communication; how do we communicate, what do we communicate, and how do we not leave anyone out, in particular, special needs populations**

Hearing Called to Order: 1300

The meeting was called to order by George Foresman, Director of the Office of Commonwealth Preparedness and Chairman of the Secure Commonwealth Panel. Mr. Foresman introduced other members of the Secure Commonwealth Panel in attendance: Colonel Wayne Huggins (Ret., VSP) and Brigadier General Manuel Flores (USA, Ret.). The following opening remarks were offered.

George Foresman: Thank you for coming. Welcome two other panel members: Brig. General Manual Flores and Retired Col Wayne Huggins. Where do we need to go with out initiatives to prepare, prevent and respond to emergencies? Critical Role- local, state citizens prepare for and respond to crisis. Man made or natural disasters/emergencies: we need to know how to respond and prevent. How to we integrate all sources to work together to respond. Secure Commonwealth plan is an ALL of us plan. Need to keep going even with the transition of government.

Brig General Flores: Thank you for coming. Has served on the panel for year and half. George done great job to look at all areas. Luckily there that have not had the recent disasters but we need to be ready. The plan is a very good plan, a good start. We need money to execute.

Col Huggins: Thanks for coming for sharing opinions about where we are and where we should be, Served on Last two panels come long way in last 4 years but we have long way to go. The word Draft is on Plan. Should always be a draft. WE will never be totally prepared. Need to keep updating. Need to work together as partnership: state, local and federal.

Chairman Foresman: This is critical: Do we have the right direction? May not be in plan but may be appendix; vision ahead and why and how to implement.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

PUBLIC COMMENT PERIOD

Paul Pokorski (Virginia Beach Fire Department):

- Liked the fact that this is a local and state perspective. Very happy that it is local partnership.
- Reflecting on what VA has gone through and the disaster that the Gulf has gone through. Appreciate that Virginia is working to make changes.
- *Chairman Foresman*: If you did not get that it as a state and local partnership then we need to strengthen that aspect.
- *Col Huggins:* Reiterated that panel has people from all over state, lots of local representation on panel.
- *Gen. Flores:* We need to get citizens more involved, need to be ready to respond. Need to have sub-plans to have citizens involved so that they can deter and be the eyes and ears. We should strengthen the deterrence theme in this plan.

Sonia Marromatis (Tyson's Food):

- Being from a small town then moving to large city, I always thought that nothing would happen in a smaller community, it does happen here.
- We need to change the mindset of smaller areas/towns. What are we doing with smaller towns?
- *Chairman Foresman:* Do you feel that we need to be more inclusive of smaller communities? Good take away is that we need to make sure that the strategy brings along smaller communities. Do you feel that our strategic plan regarding agriculture plan is good?
- *Ms. Marromatis:* Yes, absolutely.
- *Col. Huggins:* There are significant risks are in the rural areas. Lots of regional planning is going on in rural areas that contain high-risk targets. They may not seem obvious to the public, but they are happening.

Judy Riutort **(**York County Director of Emergency Management):

- Very impressed with the plan.
- Will the events down at the Gulf alter the plan? Monday morning quarterbacking?
- People assume that shelters have generators; when in fact they do not. So do you think that the issues that were revealed from Katrina (shelters, generators, etc) will alter funding priorities?
- *Chairman Foresman:* Evacuation plans are important as are shelters. However the goals should place emphasis on protective actions for areas. The special needs is a large population and we need to have plan and way to assist. We need to review the shelter-in-place, evacuation, and citizen preparedness plans (protective actions).
- *Col Huggins:* There will be funding complications as a result of hurricane. Transportation appears to big hot topic issue for voters. Oceana is another huge ticket funding item. The longer we go without event, focus goes away from prevention it goes to other areas like transportation etc.

Hui Shan Walker (City of Chesapeake Deputy Coordinator of Emergency Management):

- Excellent document. Did see the local aspect.
- COOP: Commonwealth has plan but does the local government have one; local officials need guidance for COOP.
- Performance measures: Lots of funding has gone into assessments but need to have more local involvement for measurements.
- *Chairman Foresman:* In response to the COOP issue, what you mentioned is true. Lack of COOP and COG really impacted New Orleans. People still expect local government to keep going even though infrastructure has been destroyed. We will make sure that the COOP development for all

levels is emphasized. In regards to performance measurement, people want to be able to measure results. This needs to be done at all levels.

- *Chairman Foresman:* We will work with Virginia Municipal League and the Virginia Association of Counties to strengthen local COOP plans.

Richard Childress (Isle of Wight):

- Thanks, this document makes us take a look at these types of issues
- Lots of emphasis of what the Commonwealth will offer. Does not instruct locals on what to do. Is that intended?
- After 9/11 focus was on terrorism then with Katrina the focus as on hurricanes. Please keep it as "all-hazards".
- Unfunded mandates need to be funded.
- *Chairman Foresman:* Commonwealth means Virginians, everybody. We need to clarify that it is intended for all levels of government. I understand what you mean about unfunded mandates. If it is a priority it needs to be funded. We will look into this.
- *Gen. Flores:* Things happen then we focus on that event, each event creates different impacts. We need to prioritize. Local governments need to look at their individual vulnerabilities. Need to balance money and priorities.

Tommy Lindsay **(**Citizen/VDOT [not representing views of VDOT]):

- Government and business is a big key to restoration.
- I understand that citizens are being trained to clear roads. We need to be careful where we ask untrained citizens to help. They could hurt themselves and others.
- VDOT needs to be included in coordination. VDOT is a first responder. Need to better coordinate.
- *Chairman Foresman:* Great point; all people are responders. Nobody is excluded as a responder. We just need to figure out how to coordinate. Make sure CERT program managers have clear lines of responsibility for citizens and professional responders. How do we better share info between state police, emergency agencies, VDOT, etc.? Need to make sure that we highlight the public/private partnership within the plan. Virginia is first state to have statewide inter-operability plan.

Paul Pokorski:

- Funding needs to be consistent to make changes. Don't take money from one place to give to another.

Tom Bernard (VDH):

- The term Commonwealth needs to be changed since people are not getting that it means all entities.
- Check on the legal limitations of a Commonwealth vs. state in response, etc.
- Like the Missions statement; the Vision statement is too passive it needs to be more active (active tense rather than passive tense).
- Highlight a forward-looking focus more throughout the plan.
- *Chairman Foresman:* Insightful comments. We need to make sure that there are no limitations since we are a Commonwealth based on the constitutional laws. Need to focus on future and not on fighting the past wars. Do our plans mention forward focus and revisiting and changing?
- *Col Huggins:* The first panel was created due to 9/11. Over the course of the last 4 years we have started looking at all hazards. We have actually been focusing on natural disasters repercussions (shelters, elderly, special needs) but they could also become relevant in an act of terrorism.

Dean Beler (VDH):

- Regional coordination is very helpful and needs to be woven into the plan more.
- *Chairman Foresman:* We need to better articulate the regional coordination in the plan.

Tracy Hanger (Hampton Roads Fire and Rescue):

- Well written.
- On the issues of radio interoperability, we still need funding. Communication is critical. We need to communicate to effectively do jobs.
- On the funding of the EMS system, Virginia has always under-funded EMS and lots of local governments have not addressed this. EMS helps hospitals and we need them up and running in order to help in the event of a large event.
- *Chairman Foresman:* We keep hearing this. Key people need to talk to other key people. We area aware of this. On EMS and the health system, the sub-panel has looked into this but we will look into making sure that enough time and emphasis has been placed in this area. EMS needs to be added to strategy.
- *Col Huggins:* In regards to funding, the public needs to be involved. You need to go to your senators and representatives and tell them what is needed.

Ron Collins (VA Dept of Fire Programs):

- They are offering all-hazards types of courses in the rural areas.
- Some smaller areas do not embrace planning because they don’t feel it will happen there.
- *Chairman Foresman:* Need to better educate local incident commanders on how to handle incidents.
- *Gen Flores:* You mentioned that small communities seem to lack interest. Why?
- *Mr. Collins:* Past experience with near misses, a mindset because nothing has happened there. Generally, more rural communities like the action packed training as opposed to the lecture classes. We are trying to educate that it could happen and trying to get officials involved.

Robert Rennen (Chesapeake):

- Good Commonwealth effort.
- Some rules will need to be relaxed if incident occurs.
- Communications is twofold. Radio is one, but communication with public is another. Communication needs to be a strategy within the plan.
- *Chairman Foresman:* Health is part of STARS communication program. We need to look at communicating with the public within the strategy.

Erin Sutton (VA Beach Health Dept):

- Medical Reserve Corps needs to be included.
- Medical providers need to have medications prior to event.
- Evacuation plans need to be done, need to have better parameters. Not just call 9-1-1 as is currently in their plan.
- *Chairman Foresman:* Do we have the right focus on priorities? Many legislatives proposals have gone through. In regards to medicines prior to the declaration, do what you need to do and we will cover it in the executive order. For special needs populations, calling 9-1-1 is not acceptable. Framing the issues in terms of liability and offering incentives will drive the development of comprehensive plans.
- *Gen Flores:* We will never have enough health care support.

- *Col Huggins:* Issues with immunizations have not be given enough attention. People need to be prepared to go in advance and get those in the affected area the immunizations that they need.
- *Mr. Sutton:* Local businesses need to have input. Their involvement is critical.

Secure Commonwealth Panel Final Comments

George Foresman:

- I have a take away list from this meeting.
  1. The prevention piece needs to have more focus (gangs, fire, nuclear, natural etc).
  2. Regionalism
  3. Communication: how do we communicate; what do we communicate (do not leave anyone out, special needs, etc.)?

Gen Flores:

1. Communication
2. Citizen Involvement; educate and train them properly
3. Management: put forth best effort
4. Document is not static.

The Hearing was adjourned at 1515.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Hampton Roads Convention Center - Hampton, VA
September 27. 2005
Region 5

KEY STRATEGIC ISSUES

- **Address the key areas of communications and public education**
- **Family assistance and reunification are vital services that need to be addressed**
- **Rules and regulations are vital and necessary, but should not stand in the way of getting needed resources and doing what's necessary to save lives**
- **Resources to implement strategies will be limited. Performance measures are the key to funding and implementation**

Hearing Called to Order: 1832

The meeting was called to order by George Foresman, Director of the Office of Commonwealth Preparedness and Chairman of the Secure Commonwealth Panel. Mr. Foresman introduced Brigadier General Manuel Flores (USA, Ret.)., a members of the Secure Commonwealth Panel. The following opening remarks were offered.

George Foresman: Welcome and thank you for coming. Input is critical. We received great input at earlier session today. Program today is about the road ahead. The Governor asked that the Panel look at all areas of government, what are we doing and what do we need to do to prevent, deter, prepare, recover from all types of emergencies; and better manage risks.

General Flores: Thank you for making time to go listen and help develop the Plan. The document is dynamic, not static. As we learn from incidents, we need to update and ensure that security is provided to the citizens. Money is an issue/concern but as managers we need to prioritize. We invite your comments.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

Chairman Foresman: Three key things came out of earlier today.

1. Some local officials saw this as a "Commonwealth" strategy when it is for all. We will look at changing the language.
2. Communications is key. How and what we communicate with each other?
3. Does this document offer the key strategies and places we need to go?

PUBLIC COMMENT PERIOD

Don Schindel (Private citizen, Regional Coordinator for Hospital Preparedness Committee/Central VA Hospital Coordinator)

- Concerned with communications to the public.
- The attendance at this meeting shows how they do not understand what the Commonwealth is doing.
- When we try to educate, they don't seem to take seriously.
- Preparedness needs to begin in all levels of the school system. Perhaps "Readiness Fairs".

- People assume that nothing will happen or that we already know how to respond because we have always. We need to better benefit from past experience.
- For example, evacuation out of this region. For medical evacuation a rail system would be ideal, but we do not have that option. We need a system.
- In a disaster, we do what is best for masses but end up leaving some out. Is there legislation out there that allows for treatment of the masses at the cost of others?
- *Chairman Foresman:* Focus on education and outreach is critical. Lady earlier today mentioned that the rural communities seem to lag behind in preparedness. Smaller communities were the ones that suffered the most in Katrina. We do need a better method to capture lessons learned. In a mass casualty situation, should there be a standard of care? Need to educate people that during a disaster their standards will need to shift.
- *Gen Flores:* We need to better involve the citizens.
- *Mr. Schindel:* We need to have the authority to make the decision regarding mass care at the cost of others. We need to be allowed to make judgment call. As far as education goes, can we give this presentation to school administrators to get their input about implementing this in the school system?
- *Gen Flores:* We will never have enough facilities to care for the injured in a major disaster. How far down the ladder can we go to make the decision regarding mass care?
- *Chairman Foresman:* School administrators have had push back. Maybe we need to go back and ask them what do we need to do to prepare the schools.

Elizabeth Kinnison (Office of Chief Medical Examiner):

- Need a more defined way to find family members: sick, missing, dead. We need Family Assistance Center plan that is well defined.
- Mass graves are not acceptable to public. We need to develop a better system for the dead and their family.
- The Medical Examiners Office needs to be included in drills and exercises to test the logistics of where will you put the dead, what will you do?
- Need to learn to better communicate with the Federal Government.
- *Chairman Foresman:* Family Assistance/Reunification System needs to be a strategy anda priority.

Suzanne Love (VA Dept of Health):

- Tracking dead/alive/injured people needs to be developed. It is critical.
- The VA DMAT Team, as a federal entity, cannot be used it within the Commonwealth unless it becomes a state asset.
- *Chairman Foresman:* We agree that the reunification is critical and key. We cannot allow rules and regulations to impede response and preparedness but we also need rules to operate effectively. Need to look at including this in plan. One of the strategies to look at communities preparedness; we probably need to stop and assess. Need to know what we have in capabilities. Where are we? What capacity do we have?
- *Ms. Love:* We want to be able to use this “Federal” asset (the DMAT) even though no federal declaration, only a state declaration.

Don Schindel:

- Grants tend to be focused on a particular item, people are pulled in many directions. Need leniency from Feds with grant monies?
- *Chairman Foresman:* Performance measures are key. Need to make tough choices, enhance preparedness or improve roads.
- Federal grants have benchmarks that are required. Once we achieve them, then they need to give help to do trainings.
- *Gen Flores:* You are right, get waiver for urgent needs as opposed to what the exact intend of the grant.
- *Chairman Foresman:* Don’t focus on past we will have higher degree of flexibility in the future. Incentives need to be included. Need to allow flexibility to help the masses. Liability protection.

Secure Commonwealth Panel Final Comments

Gen Flores: Great comments. You have hit the nail on the head. Education, communication and funding are key issues. Need to keep pushing these ideas.

George Foresman: On behalf of the Governors Office, thank you very much for coming out and providing your feedback. This will help us with a forward focus. Three key points: communications; resources and funding; and although the past is important, we cannot get lost in the past, we need to learn from it and come up with new ideas.

Public Comments will end at 8pm tomorrow night but you can always provide comments and insights.

The hearing was adjourned at 1948.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Chesterfield County Government Center - Chesterfield, VA
September 28, 2005
Region 1

KEY STRATEGIC ISSUES

- **Mass fatalities need to be addressed in the strategic plan**
- **Improving our capability to communicate with the public is a key strategy. This includes education and dissemination of "protective measures" (evacuation, shelter-in-place. etc.)**

Hearing Called to Order: 1302

The meeting was called to order by George Foresman, Director of the Office of Commonwealth Preparedness and Chairman of the Secure Commonwealth Panel. Mr. Foresman introduced Brigadier General Manuel Flores (USA, Ret.)., a members of the Secure Commonwealth Panel. The following opening remarks were offered.

George Foresman: Welcome, we appreciate you coming. We are here to discuss Virginia's readiness on all levels to prepare for emergencies and disasters of all kinds. In January of 2002, Gov, Warner instituted the Secure Virginia Panel to see where were and where we need to go to prepare, respond to and recover from all forms of emergencies. He wanted to develop a strategy for all of Virginia not just the "state" government and chart the path forward that we need to go down. We want the next administration to be able to pick up and continue moving forward. This project is going to be measured by the citizens. Citizens want an effective response regardless of where it is coming from. This is not a static process. It continues to grow and may always be a draft as it continues to change and grow. Three goals for today: One, an overview of the plan and strategy, a vision of road ahead and our guiding principals. Two, answer questions, have discussion and get feedback for various issues. Three, walk away with the understanding that we have the right vision/strategy for the future.

General Flores: Thank you for making time to go listen and help develop the Plan. Please express your ideas or thoughts. Please share all. Want you to feel that you are part of the plan. Communication is key, education of public is also key. We feel we have a good plan but we still need to execute and be ready.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

Chairman Foresman: The approach to the plan is all-hazards. We must be able to manage risks as opposed to specific hazards and achieve a higher level of preparedness regardless of event. The key is performance measures.

PUBLIC COMMENT PERIOD

Ed Rhodes (Virginia Fire Chiefs Association):

- More questions than comments.
    - Page 16: Dedicated funding source: what will this do to existing dedicated funding? Will this be additional or taken from funds?
    - Bullet 6: clarify

  - Bullet 9: clarify
  - Page 19: EMS initiatives. The 1st bullet taken care of in last general assembly. The 2nd bullet, there is concern about setting minimum response time, urban versus rural time is being toyed with. The 3rd and 4th bullets dealing with money.
- *Chairman Foresman:* In funding for preparedness we don't want to take away existing funds and do not want to diminish funds. We need to clarify in the plan. For regional areas, we want to move toward risk-based funding with further incentives for regional cooperation. For the full-time emergency manager, we are sensitive to state mandates. Local governments and states are going to have to start making priorities to prepare for emergencies and disasters. Will need to go back and look at the other two issues and will send letter to clarify.
- *Gen Flores:* Money will always be an issue so we need to put our best management forward to make best impact. We may need to be flexible to alter the purpose of funding to use it for the greatest need rather than intended purpose.
- *Mr. Rhodes:* Many places currently only have the minimal supplies for response. We also need money for training and fire supplies.
- *Chairman Foresman:* The point is taken for the need to make higher standards for training.

Ken Ryals (City of Emporia):

- Emergency shelters, supplies, generators etc. Is there funding/grants to get better supplies?
- *Chairman Foresman:* Protective measures need to be better looked at. We need to better educate public. If evacuation is best protective measure than do we have the capacity to do this and execute it. Are there funds available today? No. Maybe non-profits? Make sure that we have a clear implementation plan for protective measures, particularly evacuations.
- *Mr. Ryals:* New armories do not have generators for the military units.
- *Chairman Foresman:* Administrative step. We need to follow up with guard regarding their COOP.

Terry Sullivan (Hanover Sheriff Department):

- Looks great.
- Page 17 regarding first responder's intelligence. How do you know who needs to know what and when? Written requirements mentioned in plan, will this address this?
- *Chairman Foresman:* Intelligence fusion. The question today is "Who doesn't need to know?" The right information needs to get to the right people. This is about information sharing. Federal law enforcement needs to notify locals. National standard are still out there in development.
- *Mr. Sullivan:* Page 40 mentions base level preparedness (bullet 1). How will you do this?
- *Chairman Foresman:* We will use the National Preparedness Goal in all jurisdictions. It is a requirement to get homeland security funds.

Michael Todd (Area Manager for Dairy Farmers of America):

- They are concerned about agro-terrorism. They have crisis manager in each area.
- Offered reference material that might be used for Virginia plan development.
- *Chairman Foresman:* Must give this attention. We appreciate this, we might want to follow up with you on this.

Steve Ennis (VA Health Care Association):

- He is confused based on recent experiences. There was direct communication from the Federal government all the way down to hospitals. Is there a Federal to State connection to assure coordination?
- On page 23 and on page 24, WebEOC is being put forward for interoperability in hospitals. They have been working on WebEOC, but should have it piloted. VHHA needs to be part of the plan.

- Did not see any hospital representation on the fatality management task force.
- *Chairman Foresman:* This was an oversight. Chairman Foresman then asked Marcella Fierro, Chief Medical Examiner, to respond to mass fatality care.

Marcella Fierro (Chief Medical Examiner, VA):

- Virginia has statewide medical examiner system, regionalized with hierarchy of reporting.
- 13 pathologist, 8 investigators ready to travel within an hour.
- Plan based on premise that no help will be coming from the Federal government for 72 hours.
- Body collection points would be established quickly.
- We would work with social services to reconnect family members.
- There is no federal standard for looking for missing family due to emergency.
- Interoperability is a big issue. Need to better upwardly communicate with the Federal Government.

Mike Magner (VDH):

- Page 27: New initiatives. Who will be main proponent for surge capacity and who will fund it?
- *Chairman Foresman:* I don't know. I will get back with you.
- We will need to make adjustment to care policy, i.e., what is reasonable for care when there is a mass event? We will need to have flexibility to act outside the normal standard of care. Statute cannot get in the way of good decisions.

Kenny Williams (Prince George County Police Dept):

- In the 2004 grants we faced problems with justification. When request was passed through state we were then told we needed additional justification since it was going to the Federal government. Need better clarification regarding grants requirements, purchasing off the GSA? and clearer instructions to streamline process for grant funding.
- Regional efforts for all resources. We cannot be too widespread because then cannot deal with local emergency.
- *Chairman Foresman:* GSA schedule purchase, the point is well taken. Communication is the key. Concerned that information regarding these types of purchases has not gone out to all levels. For the plan, we will need to include strategies to make sure administrative processes and grant management processes are included.
- *Gen Flores:* In regards to logistics, we need to have the right product at right time at right place. Need to make sure we are coordinated with surrounding jurisdictions. Need to educate and have networking information available.

Secure Commonwealth Panel Final Comments

George Foresman:

- This is not a static process.
- We received state independent auditors report on use of Homeland Security funds. There were no reports of misuse in VA. Very proud of this fact.
- We are not doing a good job with citizen education; need to improve. Risk education.

Gen Flores: We need to continue to learn and improve during "down" time in between events. Don't get lax; get ready to act.

The hearing was adjourned at 1454.

Secure Commonwealth Initiative Strategic Plan Public Hearing
Chesterfield County Government Center - Chesterfield, VA
September 28, 2005
Region 1

KEY STRATEGIC ISSUES

- **Prevention strategies need to be addressed as part of public education**

Hearing Called to Order: 1833

The meeting was called to order by George Foresman, Director of the Office of Commonwealth Preparedness and Chairman of the Secure Commonwealth Panel. The following opening remarks were offered.

George Foresman: Welcome, we appreciate you coming. We are here to discuss Virginia's readiness on all levels to prepare for emergencies and disasters of all kinds. In January of 2002, Gov, Warner instituted the Secure Virginia Panel to see where were and where we need to go to prepare, respond to and recover from all forms of emergencies. He wanted to develop a strategy for all of Virginia not just the "state" government and chart the path forward that we need to go down. We want the next administration to be able to pick up and continue moving forward. This project is going to be measured by the citizens. Citizens want an effective response regardless of where it is coming from. This is not a static process. It continues to grow and may always be a draft as it continues to change and grow. Three goals for today: One, an overview of the plan and strategy, a vision of road ahead and our guiding principals. Two, answer questions, have discussion and get feedback for various issues. Three, walk away with the understanding that we have the right vision/strategy for the future.

Mr. Tim Lockett from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.Chairman Foresman: The overarching issues include managing risks irrespective of cause (gang, avian flu, terrorism). Do we have the structures in place to deal with all types of risks? We need to educate the public to protect themselves, prepare themselves, and take protective measures. We need to look toward the future and not get caught in past.

PUBLIC COMMENT PERIOD

Robyn Luffman (Trauma Nurse, ED Preparedness Director; VA Commonwealth University Hospital):

- Need to stress training. Hospitals tend to become business. Training needs to be better and mandated.
- *Chairman Foresman:* Do you think there is a lack of interest as far as administrators? From liability standpoint do administrators view it differently?
- *Ms. Luffman:* Probably. They will probably start placing the emphasis on other areas.
- *Chairman Foresman:* Do you feel that you are getting a good flow of information?
- *Ms. Luffman:* We are starting to see change, people are seeking information more information.

Allen Payne (Paramedic; EMS Liaison, VCUH):

- I am seeing better-prepared squads but the smaller squads do not have the means or the staff to achieve the same level as the larger units. I only have 2 weeks experience in this job.

- *Chairman Foresman:* Get 6 weeks experience then get back to me and tell me if there is an understanding with the smaller organizations on the importance of training. It is tough to get volunteers to come to training.
- *Mr. Payne:* Fair enough.

Dr. Robert Fierro (Private physician):

- Administrations in hospitals are starting to look at preparedness. They realize they will be caught and they know they need to be caught prepared and not unprepared.
- The Richmond Academy of Medicine has instituted a credentialing program. Hospital staff will know immediately, there is one universal ID card throughout Richmond area hospitals.
- *Chairman Foresman:* That is an excellent gem. This could probably be linked with the State initiative. We are working toward a standardized credentialing program within VA, we will hook you up with that effort.

Captain Grant Warren (Deputy Chief of Support for VCU Police)

- People need to be better educated and know what is out there.
- We need to get citizens to be able to take care of self for at least 72 hours.
- Feds have free training. States need to utilize it.
- Prevention needs to be applied across the board. Need appraisals of all risks and how to respond to that risk.
- Inverted hierarchy, citizens are provided with education and training so they know what needs to be done (from school, etc).
- VCU/OneCard that works for all, access control, cashier, etc.
- *Chairman Foresman:* In regards to citizen training, we agree that we do need to get the students from elementary school to colleges and universities included in this process and trained. Make sure that training can be brought home and implemented there.

Linda Price (Chesterfield Emergency Manager):

- We are headed in right direction. Leaders are listening and know that the job of emergency manager is important
- We have more money available now; we need to spend it better (more strategically).
- Challenges remain: Mass evacuations. We must continue to plan. We need citizen education prior to the event. Isolation is a difficult task that must be met within constitution.
- *Chairman Foresman:* Public Policy is focused on preparedness right now; needs to be more in the strategy.

Marcella Fierro (OCME, VA):

- Virginia has statewide medical examiner system, regionalized with hierarchy of reporting.
- 13 pathologists, 8 investigators ready to travel within an hour.
- Plan based on premise that no help will be coming from the Federal government for 72 hours.
- Body collection points would be established quickly.
- We would work with social services to reconnect family members.
- There is no federal standard for looking for missing family due to emergency.
- Interoperability is a big issue. Need to better upwardly communicate with the Federal Government.

Secure Commonwealth Panel Final Comments

George Foresman:

- Strategies are only as good as the implementation, which is a difficult task.

The hearing was adjourned at 1943.

Secure Commonwealth Initiative Strategic Plan Stakeholders Meeting
Northern Virginia Regional Council - Fairfax, VA
October 3, 2005
Region 7

KEY STRATEGIC ISSUES

- **The Commonwealth should institute a proactive programmatic information turnover and training program for security issues to ensure planning and programs do not lag due to administrative transitions.**
- **Communication and education of the public on preparedness issues must be improved**
- **Improve training and meet national security training standards**
- **The Commonwealth needs to better clarify the State coordination role of facilitating Federal assistance to a local emergency.**
- **Any new equipment acquired for security must come with corresponding training and maintenance support.**
- **The health and medical system needs more equipment, while first responders require additional staff.**
- **Horizontal and vertical information sharing amongst and between Federal, State, and local levels must be improved.**
- **Crisis communications must be coordinated to ensure regions speak with one voice.**
- **The Commonwealth should establish a statewide training program to ensure citizens fully understand the level of insurance coverage they possess against emergencies.**

Meeting Called to Order: 1730

The meeting was called to order by Dave Schwengel, of the Northern Virginia Regional Council. George Foresman, Assistant to the Governor for Commonwealth Preparedness and Chairman of the Secure Commonwealth Panel (SCP) was delayed until 1900. Mr. Schwegel introduced other members of the Secure Commonwealth Panel in attendance: The Honorable Jane Woods, Secretary of Health and Human Resources, Suzanne Spaulding, Patricia Morrissey and John Quilty.

Members of the SCP made additional opening remarks.

Ms. Spaulding:

- Mentioned that the SCI was a very inclusive process supported by input from a number of open meetings and forums

Mr. Quilty:

- Stated that the execution of the plan is the responsibility of operational personnel

The session began with introductions of those in attendance.

Mr. Geoff Nagler from Community Research Associates, Inc. presented an introductory overview of the Secure Commonwealth Initiative Strategic Plan.

COMMENT PERIOD

Sec. Woods:

- Observed that statewide elections occur on four-year rotations. She emphasized that an issue as critical as Commonwealth security should not be allowed to lose momentum during a change of administration. She felt it was important to capture the status and milestones of the process on paper. Therefore, a new administration could "hit the ground running." This Secure Commonwealth Initiative Plan is the cornerstone of the process and the legacy of each administration. The transition document should identify where we are and provide what steps need to be taken.

Pat Collins:

- When developing standards the Commonwealth needs to be very careful of what "standards" are utilized. Training needs to be coordinated with standards established on a national level by ODP.
- Page 17 – sounds like a CERT mandate – funding of those things that are mandated. Training of citizens (CERT). How are we going to do it? It is something that needs to be in strategy – but how do we do it? Benchmark – 50% in county. Citizen surveys. Large population of non-English speaking people.

Barbara Gordon:

- Training needs to be done:
  1. With multiple tools in many forms (email, radio, TV, bumper stickers)
  2. Repeatedly.
  3. At all levels.

Lucy Caldwell:

- Utilization of non-traditional ways of communicating with citizens has proven effective. Working with churches. Different groups. Are making progress – looking at other ways besides media.

Sec. Woods:

- The Commonwealth needs to use existing infrastructures and multiple vehicles. There must be a consistent message to citizens.
- Regions/locals should implement and tailor content. The State should provide the tools, content and resources.
- Training of CERTS at the state level can be addressed by things like preparedness day that get ingrained into the community.

Ms. Gordon:

- Children – get it in school. Children have been excellent conduits for anti-smoking campaigns, recycling, and ecology. Perhaps the same approach would prove effective with communicating security issues. Kids get the information home and can surmount language barriers.

Doug Scott:

- Regarding Government Operations and Funding – A lot of responsibility will fall to locality to implement. Who will do this? Localities have taken upon themselves to staff. Arlington EMA staff. Funding – Is any dedicated funding going to be made available to staff positions?

- The majority of federal dollars go to equipment. There is no capacity to assist with personnel.
- Templates are nice, but localities are so different. Difficult to have something that meets all requirements. Trust fund idea – think of funding stream to be identified.

Patti Morrissey:

- Homeland security funding allocation should be threat-based.

Tony Griffin:

- Concern that NoVA has had mandates/strong suggestions with no or little funding. May occur first year – not second. Funding federal at this point, done by population. Vital private sector operations. How is state going to do this? States and jurisdictions no longer have a direct link to DHS Secretary – all state and local communications go through Undersecretary. State needs to be engaged in dialogue with federal government. Don't see how that relationship is identified in the plan. State plays a facilitation / coordination role. Role of state in facilitating assistance to localities.

Bill MacKay:

- Federal funding buying equipment. Need to address element of human resources. Support training and exercises.
- For the long haul, focus needs to be on training and exercises of personnel.

Mr. Collins:

- UASI types of programs. Room secure systems – funded OK. What about sustainment? As soon as funding stream for programs get turned off, the program gets turned off.

George Foresman:

- Millions of dollars have been allocated to create an extraordinary capacity. What is the environment for base-line capability? Fundamentally haven't had to make choices. $200B to repair Gulf Coast coming from somewhere. $100B for war in Iraq is coming from somewhere. Look at different approach. Nice to haves are great. Gotta haves necessary. Are we ready to have this policy discussion?

Mr. Collins:

- Up until now, we have sort of been guessing. Some point need to say this is what jurisdictions need to be able to do. We threw money to buy stuff. Plan is the hard part. Now we have to make some tough decisions. What to fund. How best to use the money.

Chairman Foresman:

- From strategic standpoint: 1) How do you come up with those things – how do you coordinate with National Preparedness Goals? 2) Define how NPG best suits Virginia. Defining the end-point – federal partners have provided the first step.
- Interstate highway system – how do we take macro-strategic piece and apply it to Virginia? Flexibility to prepare for crisis events. Citizen – public education and information universal across the state? Funding for positions – provide a base level for capacity at local level. Not sure what "base-level" is.
- Risk-based analysis should be used.

Sec. Woods:

- The current security environment has rebuilt the health department system. The health and medical systems received funding for staff. Equipment is not there. Need better balancing of people and equipment. Doesn't have robust information sharing. Have basic surveillance. Recovery based on ability to capture information. Education and training component – constant – has not been funded. Once you have lost the people, can't get them back. Health departments are thinly stretched.

Suzanne Spaulding:

- It's information sharing. Health and medical not part of the stream?

Chairman Foresman:

- Health departments – certain things they can/cannot share. Working around conflicting federal guidelines. FY07 – take a group – grant guidelines HHS (people, not stuff). DHS grant (stuff, not people). Focus and compare. Can state get a better perspective on solutions set? May provide greater flexibility.

Lucy Caldwell:

- Issues on the regional level. Issues that need to be worked at regional and state level. Work very closely on daily basis. Issue could be when something happens. Who is going to be spokesperson for region? Health issues very frightening for people. Have to figure out how to solve.

Chairman Foresman:

- Shouldn't treat this region any differently than any other area of the country.

Sec. Woods:

- Been very differential to the feds in this region, almost to our detriment. Don't get information from feds in a rapid way. Fear factor is almost too large.

Jim Quilty:

- Areas attractive to terrorism. How do folks feel at things inherently cross-jurisdictional? How do you feel about processes?

Mr. Mackay:

- Good except back in March with anthrax incident. Need to get better coordination of biological incidents across region. Conflicting roles and responsibilities with Health commission and first responders, which sometimes creates conflicts.

Mr. Griffin:

- Lack of good consistent coordination with federal agencies. Federal government relies on us for the service. We have enough power to frustrate each other. Need to figure out how to work together. Feds have no experience at local level.

Ms. Morrissey:

- Information sharing – need more information on how the feds relate to the warning piece (horizontal and vertical).

Mr. Griffin:

- Made progress. Fairfax County – intelligence process post-9/11. Relationship with FBI better. Have to rely on local partners. Need to be more effective at partnership. States get more attention in capitol. The State should try to enhance facilitative role.

Chairman Foresman:

- May need to start the process and invite feds to the table. All seeking the same goal.

Mr. Griffin:

- State has served as a homeland security laboratory for the feds. 95% of the first response for federal assets in the northern Virginia area are paid for by local government. Need to leverage partnership.

Sec. Woods:

- Citizenry trust local government more than state and a lot more than federal government.

Ms. Spaulding:

- Not waiting for federal government to get act together. States and locals have a certain amount of liability.

Mr. MacKay:

- Insurance industry. State should work up common definitions of coverage (homeowners, etc) following the events of Katrian. People may think they are covered and they are not.

Sec. Woods:

- Utilities not at table with local EOCs.

Chairman Foresman:

- Cost recovery. Issue – can you get to them in a timely manner? Broader issue at bringing utilities to the table. Secretary will move on this. Regulatory process.
- Have to develop framework. 1) Help federal partners. Identify lanes. Regulatory standpoint – things regulated by states.

Secure Commonwealth Panel Final Comments.

Mr. Foresman: Apologized for being late and expressed appreciation. Stated that the SCI plan would retain the word draft in perpetuity to reflect that it is a living document and should remain so. Mr. Foresman also stated that the Governor was making legislation to codify the Office of Commonwealth Preparedness to remain as a coordinating body for security issues in the state. Both candidates for Governor are supportive of the SCI plan.

Meeting Adjourned: 2030.

Appendix A – Participant Lists

Secure Virginia Initiative Strategic Plan Public Hearing

Fairfax, VA - September 14, 2005 - 1:00 pm

NAME	AGENCY/ORGANIZATION
Panelists	
George Foresman	Governor's Office of Commonwealth Preparedness, Richmond, VA
Senator Janet Howell	Virginia State Senate, Reston, VA
Michael Neuhard	Fire Chief, Fairfax County, Fairfax, VA
Jim Quilty	Secure Commonwealth Panel
Attendees	
Donald Amos	Herndon Police Department
Leon Buckley	City of Manassas GMURS
Randall Burdetto	Department of Aviation – Virginia (DOAV)
Melvin Byrne	Virginia Department of Fire Protection
Cindi Causey	Virginia Department of Emergency Management
Cyndi Jones	DOSA – Director's Office
Anwar M. Othman	Virginia Department of Transportation – Northern Virginia
Mark Penn	City of Alexandria - Emergency Management
David Schwengel	Northern Virginia Regional Commission
Chad Weaver	Department of Aviation – Virginia (DOAV)

Secure Virginia Initiative Strategic Plan Public Hearing

Fairfax, VA - September 14, 2005 - 6:30 pm

NAME	AGENCY/ORGANIZATION
Panelists	
George Foresman	Governor’s Office of Commonwealth Preparedness
The Honorable Katherine K. Hanley	Secure Commonwealth Panel
The Honorable Jane H. Woods	Secretary of Health and Human Resources
Attendees	
Gloria Addo-Ayensu	Fairfax County Health Department
Rajaa Satouri, MD	Fairfax County Health Department
Roy Shrout	Fairfax County Office of Emergency Management
Reuben Varghese	Arlington County Public Health Division

Secure Virginia Initiative Strategic Plan Public Hearing

Christiansburg, VA – September 20, 2005 – 1:00 PM

NAME	AGENCY/ORGANIZATION
Panelists	
Robert Newman	Governor's Office of Commonwealth Preparedness
Attendees	
Donald E. Hansen	VA Department of Fire Programs
Elizabeth Nichols	Office of the Chief Medical Examiner
Sharon A. Poff	Town of Vinton
Willie Richardson	Pulaski County
Richard E. Burch, Jr.	Roanoke County Fire/Rescue
Joey Stump	Roanoke County Fire/Rescue
Chad E. Weaver	VA Department of Aviation
James R. Cox	Galax Police Department
G. Hampton	RWFD
Morris D. Reece	Near Southwest Preparedness Alliance
Larry E. Seamans	MD/VA Milk Producers Coop
Gary W. Roche	Pulaski Police Department
Bob Dix	Virginia Aviation Board
Ann Dix	Virginia Aviation Board

Secure Virginia Initiative Strategic Plan Public Hearing

Christiansburg, VA – September 20, 2005 – 6:30 PM

NAME	ORGANIZATION/AGENCY
Panelists	
Robert Newman	Governor's Office of Commonwealth Preparedness
Attendees	
Neal Turner	Montgomery County Emergency
Mike Wilson	APCO
Elizabeth Nichols	Office of the Chief Medical Examiner
Chad E. Weaver	VA Department of Aviation

Secure Virginia Initiative Strategic Plan Public Hearing

Lynchburg, VA – September 21, 2005 – 1:00 PM

NAME	ORGANIZATION/AGENCY
PANELISTS	
George Foresman	Governor's Office of Commonwealth Preparedness
ATTENDEES	
Chris Slemp	Franklin County Public Safety
Steve Eanes	Franklin County Public Safety
Gregory Wanger	Office of the Chief Medical Examiner
Charles Singleton	VSFA
Chad E. Weaver	VA Department of Aviation
Jack Jones, Jr.	Bedford County Fire/Rescue
Marvin Sheldon	Southside Community Hospital
Susan Rorrer	Nelson County
Gary Roakes	Amherst County Public Safety
Bettina Bryant	CVTC Safety Department
Joyce Waugh	Roanoke Regional Chamber

Secure Virginia Initiative Strategic Plan Public Hearing

Lynchburg, VA – September 21, 2005 – 6:30 PM

NAME	ORGANIZATION/AGENCY
Panelists	
George Foresman	Governor’s Office of Commonwealth Preparedness
Attendees	
Lee Ann Carr	Bedford Area Chamber of Commerce
Chad E. Weaver	VA Department of Aviation
Elizabeth Nichols	Office of the Chief Medical Examiner

Secure Virginia Initiative Strategic Plan Public Hearing

Culpeper, VA – September 22, 2005 – 1:00 PM

NAME	ORGANIZATION/AGENCY
Panelists	
Robert Newman	Governor's Office of Commonwealth Preparedness
Attendees	
Chad E. Weaver	VA Department of Aviation
Tom McCoy	Mary Washington Hospital
Nancy Bull	Office of the Chief Medical Examiner
Lou Hatter	VDOT/Greene County Rescue Squad
Bruce Sterling	VDEM
Gary DuBrueler	Frederick County
Jim Branch	Culpeper County Sheriffs Office
Tim Paul	Department of Criminal Justice Services
Fotini Russo	Albemarle County ECC
Tom Hanson	Charlottesville/Albemarle
Don Utz	Valleymilk Products
Bert Roby	VA Department of Fire Programs
Cindy Fincham	Culpeper Regional Hospital
Joe Lenig	Virginia Broadband, LLC
Ed Scott	House of Delegates
Roger Cooper	VA Department of Health - Emergency Preparedness
Dan Emerson	Culpeper Regional Hospital
Colleen Dawson	Faquier County Emergency Services
Philip Myer	Faquier County Emergency Services

Secure Virginia Initiative Strategic Plan Public Hearing

Hampton, VA – September 27, 2005 – 1:00 PM

NAME	ORGANIZATION/AGENCY
Panelists	
George Foresman	Governor's Office of Commonwealth Preparedness
Colonel Wayne Huggins (VSP, Ret.)	Virginia State Police Association
Brigadier General Manuel Flores (USA, Ret.)	
Attendees	
La'Ura S. Taylor, CEO	Survival Creations
Richard Childress	Isle of White County
Michelle Oblinsky	City of Chesapeake
Hui Shan Walker	City of Chesapeake
David Redinger	Tyson Food
Sonia Marromatis	Tyson Food
Tommy Lindsay	VDOT
William Ginnow	Hampton Roads MMRS
Erin Sutton	VB Health Dept
Leah Bush, MD	VA Office of the Chief Medical Examiner
Neada J. Booker	Sentara Bayside Hospital
Randall Burdette	DOAV

Secure Virginia Initiative Strategic Plan Public Hearing
Hampton, VA – September 27, 2005 – 6:30 PM

NAME	ORGANIZATION/AGENCY
Panelists	
George Foresman	Governor's Office of Commonwealth Preparedness
Brigadier General Manuel Flores (USA Ret.)	
Attendees	
Don Schindel	Central VA Hospital Coordinator
Elizabeth Kinnison	Office of the Chief Medical Examiner
Randall Burdette	Virginia Department of Aviation
Suzanne Love	VDH

Secure Virginia Initiative Strategic Plan Public Hearing
Richmond, VA – September 28, 2005 – 1:00 PM

NAME	ORGANIZATION/AGENCY
Panelists	
George Foresman	Governor's Office of Commonwealth Preparedness
Brigadier General Manuel Flores (USA Ret.)	
Attendees	
Terrance Sullivan	Hanover Sheriffs Office
Chad Weaver	Dept of Aviation
Kenny Williams	Prince George Co Police
Bernetta Barco	US Dept of Agriculture
Gilbert Lee	Prince George County
Michael Todd	Dairy Farmers of America
Ken Ryals	City of Emporia
John Trivellin	Hanover County Fire
Cindy Shelton	Chesterfield Health District – VDH
Ed Rhodes	VA Fire Chief's Association
Mark J. Dietz	VA Hospital and Healthcare Assoc
Steve Ennis	VA Hospital and Healthcare Assoc
Marcella Fierro	OCME VA
Lisa A. Clapp	Old Dominion EMS Alliance
Douglas Ford	Petersburg Fire Rescue
Mike Magner	VDH-Henrico Health District
Barry Hawkins	VA Petroleum, Convenience, and Grocery Association
Jonathan Picket	Prince Edward County Deputy Coordinator
Gregory P. Ozmar	Petersburg Police
Kimberly Johnson	City of Hopewell
Ron Mastin	County of Henrico

Secure Virginia Initiative Strategic Plan Public Hearing

Richmond, VA – September 28, 2005 – 6:30 PM

NAME	ORGANIZATION/AGENCY
Panelists	
George Foresman	Governor's Office of Commonwealth Preparedness
Attendees	
Chad E. Weaver	VA Department of Aviation
Robin Luffman	Virginia Commonwealth University
Robert Fierro	Physician
Grant J. Warren	VCU
Marcella Fierro	OCME VA

NAME	AGENCY/ORGANIZATION
Panelists	
George Foresman	Governor’s Office of Commonwealth Preparedness
The Hon. Jane Woods	Secretary of Health and Human Resources
Patti Morrissey	Secure Commonwealth Panel
Suzanne Spaulding	Secure Commonwealth Panel
Jim Quilty	Secure Commonwealth Panel
Attendees	
Pat Collins	Prince William County
Howard Cunningham	Fairfax Citizens Corps
Lucy Caldwell	VA Department of Health
Ray Hazel	Alexandria Police
Doug Scott	Arlington County Police
Bill MacKay	Fairfax County OEM
Barbara Gordon	Northern Virginia Regional Commission
Toney Griffin	Fairfax County
David Schwengel	Northern Virginia Regional Commission

Appendix K

National Strategy for Homeland Security

NATIONAL STRATEGY FOR

HOMELAND SECURITY

OFFICE OF HOMELAND SECURITY

JULY 2002

Executive Summary

This document is the first *National Strategy for Homeland Security*. The purpose of the *Strategy* is to mobilize and organize our Nation to secure the U.S. homeland from terrorist attacks. This is an exceedingly complex mission that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.[1]

People and organizations all across the United States have taken many steps to improve our security since the September 11 attacks, but a great deal of work remains. The *National Strategy for Homeland Security* will help to prepare our Nation for the work ahead in several ways. It provides direction to the federal government departments and agencies that have a role in homeland security. It suggests steps that state and local governments, private companies and organizations, and individual Americans can take to improve our security and offers incentives for them to do so. It recommends certain actions to the Congress. In this way, the *Strategy* provides a framework for the contributions that we all can make to secure our homeland.

The *National Strategy for Homeland Security* is the beginning of what will be a long struggle to protect our Nation from terrorism. It establishes a foundation upon which to organize our efforts and provides initial guidance to prioritize the work ahead. The *Strategy* will be adjusted and amended over time. We must be prepared to adapt as our enemies in the war on terrorism alter their means of attack.

Strategic Objectives

The strategic objectives of homeland security in order of priority are to:

- Prevent terrorist attacks within the United States;
- Reduce America's vulnerability to terrorism; and
- Minimize the damage and recover from attacks that do occur.

Threat and Vulnerability

Unless we act to prevent it, a new wave of terrorism, potentially involving the world's most destructive weapons, looms in America's future. It is a challenge as formidable as any ever faced by our Nation. But we are not daunted. We possess the determination and the resources to defeat our enemies and secure our homeland against the threats they pose.

One fact dominates all homeland security threat assessments: terrorists are strategic actors. They choose their targets deliberately based on the weaknesses they observe in our defenses and our preparedness. We must defend ourselves against a wide range of means and methods of attack. Our enemies are working to obtain chemical, biological, radiological, and nuclear weapons for the purpose of wreaking unprecedented damage on America. Terrorists continue to employ conventional means of attack, while at the same time gaining expertise in less traditional means, such as cyber attacks. Our society presents an almost infinite array of potential targets that can be attacked through a variety of methods.

Our enemies seek to remain invisible, lurking in the shadows. We are actively engaged in uncovering them. Al-Qaeda remains America's most immediate and serious threat despite our success in disrupting its network in Afghanistan and elsewhere. Other international terrorist organizations, as well as domestic terrorist groups, possess the will and capability to attack the United States.

Organizing for a Secure Homeland

In response to the homeland security challenge facing us, the President has proposed, and the Congress is presently considering, the most extensive reorganization of the federal government in the past fifty years. The establishment of a new Department of Homeland Security would ensure greater accountability over critical homeland security missions and unity of purpose among the agencies responsible for them.[2]

American democracy is rooted in the precepts of federalism—a system of government in which our state governments share power with federal institutions. Our structure of overlapping federal, state, and local governance—our country has more than 87,000 different jurisdictions—provides unique opportunity and challenges for our homeland security efforts. The opportunity comes from the expertise and commitment of local agencies and organizations involved in homeland security. The challenge is to develop interconnected and complementary systems that are reinforcing rather than duplicative and that ensure essential requirements are met. A national strategy requires a national effort.

State and local governments have critical roles to play in homeland security. Indeed, the closest relationship the average citizen has with government is at the local level. State and local levels of government have primary responsibility for funding, preparing, and operating the emergency services that would respond in the event of a terrorist attack. Local units are the first to respond, and the last to leave the scene. All disasters are ultimately local events.

The private sector—the Nation's principal provider of goods and services and owner of 85 percent of our infrastructure—is a key homeland security partner. It has a wealth of information that is important to the task of protecting the United States from terrorism. Its creative genius will develop the information systems, vaccines, detection devices, and other technologies and innovations that will secure our homeland.

An informed and proactive citizenry is an invaluable asset for our country in times of war and peace. Volunteers enhance community coordination and action, whether at the national or local level. This coordination will prove critical as we work to build the communication and delivery systems indispensable to our national effort to detect, prevent, and, if need be, respond to terrorist attack.

Critical Mission Areas

The *National Strategy for Homeland Security* aligns and focuses homeland security functions into six critical mission areas: intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response. The first three mission areas focus primarily on preventing terrorist attacks; the next two on reducing our Nation's vulnerabilities; and the final one on minimizing the damage and recovering from attacks that do occur. The *Strategy* provides a framework to align the resources of the federal budget directly to the task of securing the homeland.

Intelligence and Warning. Terrorism depends on surprise. With it, a terrorist attack has the potential to do massive damage to an unwitting and unprepared target. Without it, the terrorists stand a good chance of being preempted by authorities, and even if they are not, the damage that results from their attacks is likely to be less severe. The United States will take every necessary action to avoid being surprised by another terrorist attack. We must have an intelligence and warning system that can detect terrorist activity before it manifests itself in an attack so that proper preemptive, preventive, and protective action can be taken.

The *National Strategy for Homeland Security* identifies five major initiatives in this area:

- Enhance the analytic capabilities of the FBI;
- Build new capabilities through the Information Analysis and Infrastructure Protection Division of the proposed Department of Homeland Security;
- Implement the Homeland Security Advisory System;
- Utilize dual-use analysis to prevent attacks; and
- Employ "red team" techniques.

Border and Transportation Security. America historically has relied heavily on two vast oceans and two friendly neighbors for border security, and on the private sector for most forms of domestic transportation security. The increasing mobility and destructive potential of modern terrorism has required the United States to rethink and renovate fundamentally its systems for border and transportation security. Indeed, we must now begin to conceive of border security and transportation security as fully integrated requirements because our domestic transportation systems are inextricably intertwined with the global transport infrastructure. Virtually every community in America is connected to the global transportation network by the seaports, airports, highways, pipelines, railroads, and waterways that move people and goods into, within, and out of the Nation. We must therefore promote the efficient and reliable flow of people, goods, and services across borders, while preventing terrorists from using transportation conveyances or systems to deliver implements of destruction.

The *National Strategy for Homeland Security* identifies six major initiatives in this area:

- Ensure accountability in border and transportation security;
- Create "smart borders";
- Increase the security of international shipping containers;
- Implement the Aviation and Transportation Security Act of 2001;
- Recapitalize the U.S. Coast Guard; and
- Reform immigration services.

The President proposed to Congress that the principal border and transportation security agencies—the Immigration and Naturalization Service, the U.S. Customs Service, the U.S. Coast Guard, the Animal and Plant Health Inspection Service, and the

Transportation Security Agency—be transferred to the new Department of Homeland Security. This organizational reform will greatly assist in the implementation of all the above initiatives.

Domestic Counterterrorism. The attacks of September 11 and the catastrophic loss of life and property that resulted have redefined the mission of federal, state, and local law enforcement authorities. While law enforcement agencies will continue to investigate and prosecute criminal activity, they should now assign priority to preventing and interdicting terrorist activity within the United States. The Nation's state and local law enforcement officers will be critical in this effort. Our Nation will use all legal means—both traditional and nontraditional—to identify, halt, and, where appropriate, prosecute terrorists in the United States. We will pursue not only the individuals directly involved in terrorist activity but also their sources of support: the people and organizations that knowingly fund the terrorists and those that provide them with logistical assistance.

Effectively reorienting law enforcement organizations to focus on counterterrorism objectives requires decisive action in a number of areas. The *National Strategy for Homeland Security* identifies six major initiatives in this area:

- Improve intergovernmental law enforcement coordination;
- Facilitate apprehension of potential terrorists;
- Continue ongoing investigations and prosecutions;
- Complete FBI restructuring to emphasize prevention of terrorist attacks;
- Target and attack terrorist financing; and
- Track foreign terrorists and bring them to justice.

Protecting Critical Infrastructure and Key Assets. Our society and modern way of life are dependent on networks of infrastructure—both physical networks such as our energy and transportation systems and virtual networks such as the Internet. If terrorists attack one or more pieces of our critical infrastructure, they may disrupt entire systems and cause significant damage to the Nation. We must therefore improve protection of the individual pieces and interconnecting systems that make up our critical infrastructure. Protecting America's critical infrastructure and key assets will not only make us more secure from terrorist attack, but will also reduce our vulnerability to natural disasters, organized crime, and computer hackers.

America's critical infrastructure encompasses a large number of sectors. The U.S. government will seek to deny terrorists the opportunity to inflict lasting harm to our Nation by protecting the assets, systems, and functions vital to our national security, governance, public health and safety, economy, and national morale.

The *National Strategy for Homeland Security* identifies eight major initiatives in this area:

- Unify America's infrastructure protection effort in the Department of Homeland Security;
- Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets;
- Enable effective partnership with state and local governments and the private sector;
- Develop a national infrastructure protection plan;
- Secure cyberspace;
- Harness the best analytic and modeling tools to develop effective protective solutions;
- Guard America's critical infrastructure and key assets against "inside" threats; and
- Partner with the international community to protect our transnational infrastructure.

Defending against Catastrophic Threats. The expertise, technology, and material needed to build the most deadly weapons known to mankind—including chemical, biological, radiological, and nuclear weapons—are spreading inexorably. If our enemies acquire these weapons, they are likely to try to use them. The consequences of such an attack could be far more devastating than those we suffered on September 11—a chemical, biological, radiological, or nuclear terrorist attack in the United States could cause large numbers of casualties, mass psychological disruption, contamination and significant economic damage, and could overwhelm local medical capabilities.

Currently, chemical, biological, radiological, and nuclear detection capabilities are modest and response capabilities are dispersed throughout the country at every level of government. While current arrangements have proven adequate for a variety of natural disasters and even the September 11 attacks, the threat of terrorist attacks using chemical, biological, radiological, and nuclear weapons requires new approaches, a focused strategy, and a new organization.

The *National Strategy for Homeland Security* identifies six major initiatives in this area:

- Prevent terrorist use of nuclear weapons through better sensors and procedures;

- Detect chemical and biological materials and attacks;
- Improve chemical sensors and decontamination techniques;
- Develop broad spectrum vaccines, antimicrobials, and antidotes;
- Harness the scientific knowledge and tools to counter terrorism; and
- Implement the Select Agent Program.

Emergency Preparedness and Response. We must prepare to minimize the damage and recover from any future terrorist attacks that may occur despite our best efforts at prevention. An effective response to a major terrorist incident—as well as a natural disaster—depends on being prepared. Therefore, we need a comprehensive national system to bring together and coordinate all necessary response assets quickly and effectively. We must plan, equip, train, and exercise many different response units to mobilize without warning for any emergency.

Many pieces of this national emergency response system are already in place. America's first line of defense in the aftermath of any terrorist attack is its first responder community—police officers, firefighters, emergency medical providers, public works personnel, and emergency management officials. Nearly three million state and local first responders regularly put their lives on the line to save the lives of others and make our country safer.

Yet multiple plans currently govern the federal government's support of first responders during an incident of national significance. These plans and the government's overarching policy for counterterrorism are based on an artificial and unnecessary distinction between "crisis management" and "consequence management." Under the President's proposal, the Department of Homeland Security will consolidate federal response plans and build a national system for incident management in cooperation with state and local government. Our federal, state, and local governments would ensure that all response personnel and organizations are properly equipped, trained, and exercised to respond to all terrorist threats and attacks in the United States. Our emergency preparedness and response efforts would also engage the private sector and the American people.

The *National Strategy for Homeland Security* identifies twelve major initiatives in this area:

- Integrate separate federal response plans into a single all-discipline incident management plan;
- Create a national incident management system;
- Improve tactical counterterrorist capabilities;
- Enable seamless communication among all responders;
- Prepare health care providers for catastrophic terrorism;
- Augment America's pharmaceutical and vaccine stockpiles;
- Prepare for chemical, biological, radiological, and nuclear decontamination;
- Plan for military support to civil authorities;
- Build the Citizen Corps;
- Implement the First Responder Initiative of the Fiscal Year 2003 Budget;
- Build a national training and evaluation system; and
- Enhance the victim support system.

The Foundations of Homeland Security

The *National Strategy for Homeland Security* also describes four foundations—unique American strengths that cut across all of the mission areas, across all levels of government, and across all sectors of our society. These foundations—law, science and technology, information sharing and systems, and international cooperation—provide a useful framework for evaluating our homeland security investments across the federal government.

Law. Throughout our Nation's history, we have used laws to promote and safeguard our security and our liberty. The law will both provide mechanisms for the government to act and will define the appropriate limits of action.

The *National Strategy for Homeland Security* outlines legislative actions that would help enable our country to fight the war on terrorism more effectively. New federal laws should not preempt state law unnecessarily or overly federalize the war on terrorism. We should guard scrupulously against incursions on our freedoms.

The *Strategy* identifies twelve major initiatives in this area:

Federal level

- Enable critical infrastructure information sharing;
- Streamline information sharing among intelligence and law enforcement agencies;

- Expand existing extradition authorities;
- Review authority for military assistance in domestic security;
- Revive the President's reorganization authority; and
- Provide substantial management flexibility for the Department of Homeland Security.

State level

- Coordinate suggested minimum standards for state driver's licenses;
- Enhance market capacity for terrorism insurance;
- Train for prevention of cyber attacks;
- Suppress money laundering;
- Ensure continuity of the judiciary; and
- Review quarantine authorities.

Science and Technology. The Nation's advantage in science and technology is a key to securing the homeland. New technologies for analysis, information sharing, detection of attacks, and countering chemical, biological, radiological, and nuclear weapons will help prevent and minimize the damage from future terrorist attacks. Just as science has helped us defeat past enemies overseas, so too will it help us defeat the efforts of terrorists to attack our homeland and disrupt our way of life.

The federal government is launching a systematic national effort to harness science and technology in support of homeland security. We will build a national research and development enterprise for homeland security sufficient to mitigate the risk posed by modern terrorism. The federal government will consolidate most federally funded homeland security research and development under the Department of Homeland Security to ensure strategic direction and avoid duplicative efforts. We will create and implement a long-term research and development plan that includes investment in revolutionary capabilities with high payoff potential. The federal government will also seek to harness the energy and ingenuity of the private sector to develop and produce the devices and systems needed for homeland security.

The *National Strategy for Homeland Security* identifies eleven major initiatives in this area:

- Develop chemical, biological, radiological, and nuclear countermeasures;
- Develop systems for detecting hostile intent;
- Apply biometric technology to identification devices;
- Improve the technical capabilities of first responders;
- Coordinate research and development of the homeland security apparatus;
- Establish a national laboratory for homeland security;
- Solicit independent and private analysis for science and technology research;
- Establish a mechanism for rapidly producing prototypes;
- Conduct demonstrations and pilot deployments;
- Set standards for homeland security technology; and
- Establish a system for high-risk, high-payoff homeland security research.

Information Sharing and Systems. Information systems contribute to every aspect of homeland security. Although American information technology is the most advanced in the world, our country's information systems have not adequately supported the homeland security mission. Databases used for federal law enforcement, immigration, intelligence, public health surveillance, and emergency management have not been connected in ways that allow us to comprehend where information gaps or redundancies exist. In addition, there are deficiencies in the communications systems used by states and municipalities throughout the country; most state and local first responders do not use compatible communications equipment. To secure the homeland better, we must link the vast amounts of knowledge residing within each government agency while ensuring adequate privacy.

The *National Strategy for Homeland Security* identifies five major initiatives in this area:

- Integrate information sharing across the federal government;
- Integrate information sharing across state and local governments, private industry, and citizens;
- Adopt common "meta-data" standards for electronic information relevant to homeland security;
- Improve public safety emergency communications; and
- Ensure reliable public health information.

International Cooperation. In a world where the terrorist threat pays no respect to traditional boundaries, our strategy for homeland security cannot stop at our borders. America must pursue a sustained, steadfast, and systematic international agenda to counter the global terrorist threat and improve our homeland security. Our international anti-terrorism campaign has made significant progress since September 11. The full scope of these activities will be further described in the forthcoming *National Security Strategy of the United States* and the *National Strategy for Combating Terrorism*. The *National Strategy for Homeland Security* identifies nine major initiatives in this area:

- Create "smart borders";
- Combat fraudulent travel documents;
- Increase the security of international shipping containers;
- Intensify international law enforcement cooperation;
- Help foreign nations fight terrorism;
- Expand protection of transnational critical infrastructure;
- Amplify international cooperation on homeland security science and technology;
- Improve cooperation in response to attacks; and
- Review obligations to international treaties and law.

Costs of Homeland Security

The national effort to enhance homeland security will yield tremendous benefits and entail substantial financial and other costs. Benefits include reductions in the risk of attack and their potential consequences. Costs include not only the resources we commit to homeland security but also the delays to commerce and travel. The United States spends roughly $100 billion per year on homeland security. This figure includes federal, state, and local law enforcement and emergency services, but excludes most funding for the armed forces.

The responsibility of providing homeland security is shared between federal, state and local governments, and the private sector. In many cases, sufficient incentives exist in the private market to supply protection. Government should fund only those homeland security activities that are not supplied, or are inadequately supplied, in the market. Cost sharing between different levels of government should reflect the principles of federalism. Many homeland security activities, such as intelligence gathering and border security, are properly accomplished at the federal level. In other circumstances, such as with first responder capabilities, it is more appropriate for state and local governments to handle these responsibilities.

Conclusion: Priorities for the Future

The *National Strategy for Homeland Security* sets a broad and complex agenda for the United States. The *Strategy* has defined many different goals that need to be met, programs that need to be implemented, and responsibilities that need to be fulfilled. But creating a strategy is, in many respects, about setting priorities—about recognizing that some actions are more critical or more urgent than others.

The President's Fiscal Year 2003 Budget proposal, released in February 2002, identified four priority areas for additional resources and attention in the upcoming year:

- Support first responders;
- Defend against bioterrorism;
- Secure America's borders; and
- Use 21st-century technology to secure the homeland.

Work has already begun on the President's Fiscal Year 2004 Budget. Assuming the Congress passes legislation to implement the President's proposal to create the Department of Homeland Security, the Fiscal Year 2004 Budget will fully reflect the reformed organization of the executive branch for homeland security. That budget will have an integrated and simplified structure based on the six critical mission areas defined by the *Strategy*. Furthermore, at the time the *National Strategy for Homeland Security* was published, it was expected that the Fiscal Year 2004 Budget would attach priority to the following specific items for substantial support:

- Enhance the analytic capabilities of the FBI;
- Build new capabilities through the Information Analysis and Infrastructure Protection Division of the proposed Department of Homeland Security;
- Create "smart borders";
- Improve the security of international shipping containers;
- Recapitalize the U.S. Coast Guard;
- Prevent terrorist use of nuclear weapons through better sensors and procedures;

- Develop broad spectrum vaccines, antimicrobials, and antidotes; and
- Integrate information sharing across the federal government.

In the intervening months, the executive branch will prepare detailed implementation plans for these and many other initiatives contained within the *National Strategy for Homeland Security*. These plans will ensure that the taxpayers' money is spent only in a manner that achieves specific objectives with clear performance-based measures of effectiveness.

[1] The *National Strategy for Homeland Security* defines "State" to mean "any state of the United States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, the Canal Zone, the Commonwealth of the Northern Mariana Islands, or the trust territory of the Pacific Islands." The *Strategy* defines "local government" as "any county, city, village, town, district, or other political subdivision of any state, any Native American tribe or authorized tribal organization, or Alaska native village or organization, and includes any rural community or unincorporated town or village or any other public entity for which an application for assistance is made by a state or political subdivision thereof."

[2] The distribution of the *National Strategy for Homeland Security* coincides with Congress' consideration of the President's proposal to establish a Department of Homeland Security. The *Strategy* refers to a "Department of Homeland Security" only to provide the strategic vision for the proposed Department and not to assume any one part of the President's proposal will or will not be signed into law.

Appendix L

National Strategy to Secure Cyberspace

THE NATIONAL STRATEGY TO

SECURE CYBERSPACE

FEBRUARY 2003

Executive Summary

Our Nation's critical infrastructures are composed of public and private institutions in the sectors of agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is their nervous system—the control system of our country. Cyberspace is composed of hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that allow our critical infrastructures to work. Thus, the healthy functioning of cyberspace is essential to our economy and our national security.

This *National Strategy to Secure Cyberspace* is part of our overall effort to protect the Nation. It is an implementing component of the *National Strategy for Homeland Security* and is complemented by a *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*. The purpose of this document is to engage and empower Americans to secure the portions of cyberspace that they own, operate, control, or with which they interact. Securing cyberspace is a difficult strategic challenge that requires coordinated and focused effort from our entire society—the federal government, state and local governments, the private sector, and the American people.

The *National Strategy to Secure Cyberspace* outlines an initial framework for both organizing and prioritizing efforts. It provides direction to the federal government departments and agencies that have roles in cyberspace security. It also identifies steps that state and local governments, private companies and organizations, and individual Americans can take to improve our collective cybersecurity. The *Strategy* highlights the role of public-private engagement. The document provides a framework for the contributions that we all can make to secure our parts of cyberspace. The dynamics of cyberspace will require adjustments and amendments to the *Strategy* over time.

The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation states difficult, a task which often occurs only after the fact, if at all. Therefore, the *National Strategy to Secure Cyberspace* helps reduce our Nation's vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them.

Strategic Objectives

Consistent with the *National Strategy for Homeland Security*, the strategic objectives of this *National Strategy to Secure Cyberspace* are to:

- Prevent cyber attacks against America's critical infrastructures;
- Reduce national vulnerability to cyber attacks; and
- Minimize damage and recovery time from cyber attacks that do occur.

Threat and Vulnerability

Our economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work. These computer networks also control physical objects such as electrical transformers, trains, pipeline pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace.

A spectrum of malicious actors can and do conduct attacks against our critical information infrastructures. Of primary concern is the threat of organized cyber attacks capable of causing debilitating disruption to our Nation's critical infrastructures, economy, or national security. The required technical sophistication to carry out such an attack is high—and partially explains the lack of a debilitating attack to date. We should not, however, be too sanguine. There have been instances where organized attackers have exploited vulnerabilities that may be indicative of more destructive capabilities.

Uncertainties exist as to the intent and full technical capabilities of several observed attacks. Enhanced cyber threat analysis is needed to address long-term trends related to threats and vulnerabilities. What is known is that the attack tools and methodologies are becoming widely available, and the technical capability and sophistication of users bent on causing havoc or disruption is improving.

In peacetime America's enemies may conduct espionage on our Government, university research centers, and private companies. They may also seek to prepare for cyber strikes during a confrontation by mapping U.S. information systems, identifying key targets, and lacing our infrastructure with back doors and other means of access. In wartime or crisis, adversaries may seek to intimidate the Nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems.

Cyber attacks on United States information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructures.

The Government Role in Securing Cyberspace

In general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where federal government response is most appropriate and justified. Looking inward, providing continuity of government requires ensuring the safety of its own cyber infrastructure and those assets required for supporting its essential missions and services. Externally, a government role in cybersecurity is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems; cases in which governments operate in the absence of private sector forces; resolution of incentive problems that lead to under provisioning of critical shared resources; and raising awareness.

Public-private engagement is a key component of our Strategy to secure cyberspace. This is true for several reasons. Public-private partnerships can usefully confront coordination problems. They can significantly enhance information exchange and cooperation. Public-private engagement will take a variety of forms and will address awareness, training, technological improvements, vulnerability remediation, and recovery operations.

A federal role in these and other cases is only justified when the benefits of intervention outweigh the associated costs. This standard is especially important in cases where there are viable private sector solutions for addressing any potential threat or vulnerability. For each case, consideration should be given to the broad-based costs and impacts of a given government action, versus other alternative actions, versus non-action, taking into account any existing or future private solutions.

Federal actions to secure cyberspace are warranted for purposes including: forensics and attack attribution, protection of networks and systems critical to national security, indications and warnings, and protection against organized attacks capable of inflicting debilitating damage to the economy. Federal activities should also support research and technology development that will enable the private sector to better secure privately-owned portions of the Nation's critical infrastructure.

Department of Homeland Security and Cyberspace Security

On November 25, 2002, President Bush signed legislation creating the Department of Homeland Security (DHS). This new cabinet-level department will unite 22 federal entities for the common purpose of improving our homeland security. The Secretary of DHS will have important responsibilities in cyberspace security. These responsibilities include:

- Developing a comprehensive national plan for securing the key resources and critical infrastructure of the United States;
- Providing crisis management in response to attacks on critical information systems;
- Providing technical assistance to the private sector and other government entities with respect to emergency recovery plans for failures of critical information systems;
- Coordinating with other agencies of the federal government to provide specific warning information and advice about appropriate protective measures and countermeasures to state, local, and nongovernmental organizations including

the private sector, academia, and the public; and

- Performing and funding research and development along with other agencies that will lead to new scientific understanding and technologies in support of homeland security.

Consistent with these responsibilities, DHS will become a federal center of excellence for cybersecurity and provide a focal point for federal outreach to state, local, and nongovernmental organizations including the private sector, academia, and the public.

Critical Priorities for Cyberspace Security

The *National Strategy to Secure Cyberspace* articulates five national priorities including:

I. A National Cyberspace Security Response System;

II. A National Cyberspace Security Threat and Vulnerability Reduction Program;

III. A National Cyberspace Security Awareness and Training Program;

IV. Securing Governments' Cyberspace; and

V. National Security and International Cyberspace Security Cooperation.

The first priority focuses on improving our response to cyber incidents and reducing the potential damage from such events. The second, third, and fourth priorities aim to reduce threats from, and our vulnerabilities to, cyber attacks. The fifth priority is to prevent cyber attacks that could impact national security assets and to improve the international management of and response to such attacks.

Priority I: A National Cyberspace Security Response System

Rapid identification, information exchange, and remediation can often mitigate the damage caused by malicious cyberspace activity. For those activities to be effective at a national level, the United States needs a partnership between government and industry to perform analyses, issue warnings, and coordinate response efforts. Privacy and civil liberties must be protected in the process. Because no cybersecurity plan can be impervious to concerted and intelligent attack, information systems must be able to operate while under attack and have the resilience to restore full operations quickly.

The *National Strategy to Secure Cyberspace* identifies eight major actions and initiatives for cyberspace security response:

1. Establish a public-private architecture for responding to national-level cyber incidents;

2. Provide for the development of tactical and strategic analysis of cyber attacks and vulnerability assessments;

3. Encourage the development of a private sector capability to share a synoptic view of the health of cyberspace;

4. Expand the Cyber Warning and Information Network to support the role of DHS in coordinating crisis management for cyberspace security;

5. Improve national incident management;

6. Coordinate processes for voluntary participation in the development of national public-private continuity and contingency plans;

7. Exercise cybersecurity continuity plans for federal systems; and

8. Improve and enhance public-private information sharing involving cyber attacks, threats, and vulnerabilities.

Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program

By exploiting vulnerabilities in our cyber systems, an organized attack may endanger the security of our Nation's critical infrastructures. The vulnerabilities that most threaten cyberspace occur in the information assets of critical infrastructure enterprises themselves and their external supporting structures, such as the mechanisms of the Internet. Lesser-secured sites on the interconnected network of networks also present potentially significant exposures to cyber attacks. Vulnerabilities result from weaknesses in technology and because of improper implementation and oversight of technological products.

The *National Strategy to Secure Cyberspace* identifies eight major actions and initiatives to reduce threats and related vulnerabilities:

1. Enhance law enforcement's capabilities for preventing and prosecuting cyberspace attacks;
2. Create a process for national vulnerability assessments to better understand the potential consequences of threats and vulnerabilities;
3. Secure the mechanisms of the Internet by improving protocols and routing;
4. Foster the use of trusted digital control systems/supervisory control and data acquisition systems;
5. Reduce and remediate software vulnerabilities;
6. Understand infrastructure interdependencies and improve the physical security of cyber systems and telecommunications;
7. Prioritize federal cybersecurity research and development agendas; and
8. Assess and secure emerging systems.

Priority III: A National Cyberspace Security Awareness and Training Program

Many cyber vulnerabilities exist because of a lack of cybersecurity awareness on the part of computer users, systems administrators, technology developers, procurement officials, auditors, chief information officers (CIOs), chief executive officers, and corporate boards. Such awareness-based vulnerabilities present serious risks to critical infrastructures regardless of whether they exist within the infrastructure itself. A lack of trained personnel and the absence of widely accepted, multi-level certification programs for cybersecurity professionals complicate the task of addressing cyber vulnerabilities.

The *National Strategy to Secure Cyberspace* identifies four major actions and initiatives for awareness, education, and training:

1. Promote a comprehensive national awareness program to empower all Americans—businesses, the general workforce, and the general population—to secure their own parts of cyberspace;
2. Foster adequate training and education programs to support the Nation's cybersecurity needs;
3. Increase the efficiency of existing federal cybersecurity training programs; and
4. Promote private-sector support for well-coordinated, widely recognized professional cybersecurity certifications.

Priority IV: Securing Governments' Cyberspace

Although governments administer only a minority of the Nation's critical infrastructure computer systems, governments at all levels perform essential services in the agriculture, food, water, public health, emergency services, defense, social welfare, information and telecommunications, energy, transportation, banking and finance, chemicals, and postal and shipping sectors that depend upon cyberspace for their delivery. Governments can lead by example in cyberspace security, including fostering a marketplace for more secure technologies through their procurement.

The *National Strategy to Secure Cyberspace* identifies five major actions and initiatives for the securing of governments' cyberspace:

1. Continuously assess threats and vulnerabilities to federal cyber systems;
2. Authenticate and maintain authorized users of federal cyber systems;
3. Secure federal wireless local area networks;
4. Improve security in government outsourcing and procurement; and
5. Encourage state and local governments to consider establishing information technology security programs and participate in information sharing and analysis centers with similar governments.

Priority V: National Security and International Cyberspace Security Cooperation

America's cyberspace links the United States to the rest of the world. A network of networks spans the planet, allowing malicious actors on one continent to act on systems thousands of miles away. Cyber attacks cross borders at light speed, and discerning the source of malicious activity is difficult. America must be capable of safeguarding and defending its critical systems and networks. Enabling our ability to do so requires a system of international cooperation to facilitate information sharing, reduce vulnerabilities, and deter malicious actors.

The *National Strategy to Secure Cyberspace* identifies six major actions and initiatives to strengthen U.S. national security and international cooperation:

1. Strengthen cyber-related counterintelligence efforts;
2. Improve capabilities for attack attribution and response;
3. Improve coordination for responding to cyber attacks within the U.S. national security community;
4. Work with industry and through international organizations to facilitate dialogue and partnerships among international public and private sectors focused on protecting information infrastructures and promoting a global "culture of security;"

5. Foster the establishment of national and international watch-and-warning networks to detect and prevent cyber attacks as they emerge; and

6. Encourage other nations to accede to the Council of Europe Convention on Cybercrime, or to ensure that their laws and procedures are at least as comprehensive.

A National Effort

Protecting the widely distributed assets of cyberspace requires the efforts of many Americans. The federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that organizations outside the federal government take the lead in many of these efforts. Every American who can contribute to securing part of cyberspace is encouraged to do so. The federal government invites the creation of, and participation in, public-private partnerships to raise cybersecurity awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations.

People and organizations across the United States have already taken steps to improve cyberspace security. On September 18, 2002, many private-sector entities released plans and strategies for securing their respective infrastructures. The Partnership for Critical Infrastructure Security has played a unique role in facilitating private-sector contributions to this Strategy. Inputs from the critical sector's themselves can be found at **http://www.pcis.org**. (These documents were not subject to government approval.)

These comprehensive infrastructure plans describe the strategic initiatives of various sectors, including:

- Banking and Finance;
- Insurance;
- Chemical;
- Oil and Gas;
- Electric;
- Law Enforcement;
- Higher Education;
- Transportation (Rail);
- Information Technology and Telecommunications; and
- Water.

As each of the critical infrastructure sectors implements these initiatives, threats and vulnerabilities to our infrastructures will be reduced.

For the foreseeable future two things will be true: America will rely upon cyberspace and the federal government will seek a continuing broad partnership with the private sector to develop, implement, and refine a *National Strategy to Secure Cyberspace*.

Appendix M

Interim National Infrastructure Protection Plan

Interim National Infrastructure Protection Plan

February 2005

Homeland Security

1. Introduction

Protecting our Nation's critical infrastructure and key resources (CI/KR) is vital to our national security, economic vitality, and way of life. Attacks on critical infrastructure could disrupt the direct functioning of key business and government activities, facilities, and systems, as well as have cascading effects throughout the Nation's economy and society. Furthermore, direct attacks on individual key assets could result not only in large-scale human casualties and property destruction, but also in profound damage to national prestige, morale, and confidence.

To provide a consistent, unifying structure for integrating critical infrastructure protection (CIP) efforts into a national program, the Department of Homeland Security (DHS) is developing the National Infrastructure Protection Plan (NIPP). Development of the NIPP is an ongoing, evolving process that requires the participation of all stakeholders from the private sector, State, local, and tribal entities, and the Federal Government. The NIPP outlines how DHS and its stakeholders will develop and implement the national effort to protect infrastructures across all sectors. As these CIP efforts are developed, implemented, and refined, the NIPP will be updated to reflect this progress.

The national CIP program will be an ongoing effort to protect the Nation's CI/KR. As one of the initial steps in this program, DHS and the Sector-Specific Agencies (SSAs) will share and discuss this NIPP with critical stakeholders to further ensure its effectiveness and success. Stakeholder perspectives are essential for a comprehensive NIPP supported by effective Sector-Specific Plans (SSPs) that will detail the application of the risk management framework to each of the 17 sectors. As such, the SSAs will work with their stakeholders to develop and implement the SSPs, so that protective programs and limited public and private resources are targeted toward the most critical assets within and across sectors. Success will be achieved by working together through public and private sector partnerships to identify, prioritize, and protect the Nation's CI/KR.

1.1 Purpose of the NIPP

The events of September 11, 2001 demonstrated our Nation's vulnerability to terrorist attacks. Protection of CI/KR requires knowledge of terrorist tactics and targets, combined with a comprehensive understanding of CI/KR vulnerabilities and the protective measures that can effectively eliminate or mitigate those vulnerabilities. However, even with all of the resources of the United States, it is not possible to protect all assets against every possible type of terrorist attack. The Nation's CIP program must prioritize protection across sectors, so that resources are applied where they offer the most benefit for reducing vulnerability, deterring threats, and minimizing consequences of attacks. This is an effort that requires the integrated, coordinated support of Federal departments and agencies; State, local, and tribal entities; and public and private sector asset owners and operators.

The Interim NIPP is based upon a risk management framework that takes into account threats, vulnerabilities, and consequences when prioritizing CI/KR protection activities. It provides an integrated, comprehensive approach to addressing physical, cyber, and human threats and vulnerabilities to address the full range of risks to the Nation.

The Interim NIPP is the Base Plan that provides the framework and sets the direction for implementing this coordinated, national effort. It provides a roadmap for identifying CI/KR assets, assessing vulnerabilities, prioritizing assets, and implementing protection measures in each infrastructure sector. For each sector, the NIPP will delineate roles and responsibilities among Federal, State, local, tribal, and

About the Interim NIPP

- **Why is this version "interim?"** This document provides the starting point for developing the national, cross-sector plan for critical infrastructure protection.

  The national and sector-specific programs that will be implemented under this Interim Plan vary widely in development and progress—some have been successfully operating for years, while others were more recently established. The Interim NIPP builds on the existing base, while acknowledging the need to expand dialogue and partnerships with the private sector and other stakeholders to create an integrated, national CIP program.

- **What does the Interim Plan do?** This first iteration of the Plan takes the principles of the National Strategy for Homeland Security (DHS, July 2002) to the next level to ensure consistent and comprehensive identification of assets, assessment of vulnerabilities, and prioritization of assets to guide the effective implementation of protective programs.

  This Base Plan identifies the general roles and responsibilities for each set of stakeholders, highlights best practices and initiatives already underway, and introduces features, such as metrics and stakeholder engagement, for ensuring that the program is successful. It also addresses the need for identifying market-based incentives and other mechanisms to encourage voluntary implementation as well as protecting sensitive business information.

- **What does the Interim Plan NOT do?** It does not substitute for the ongoing partnerships among DHS, the Sector-Specific Agencies, other Federal departments and agencies, the private sector, and State, local, and tribal entities.

  This Interim Plan is the starting point for building the national program and for initiating extensive dialogue with State, local, and tribal entities as well as private sector stakeholders to obtain their perspectives on protecting critical infrastructure.

- **What's next?** DHS, the Sector-Specific Agencies, and other Federal departments and agencies will work with the private sector and State, local, and tribal entities to further refine stakeholder roles and responsibilities and implement the NIPP (Base Plan) and the Sector-Specific Plans (SSPs) that will become annexes to the NIPP.

  The specific steps will be delineated in an implementation strategy developed by DHS. The results of these implementation efforts will be reflected in the next version of the NIPP, which will be issued within 270 days of issuance of this interim document.

private sector stakeholders in carrying out these activities, with DHS as the lead agency and single point of accountability and coordination.

1.2 Organization and Scope

In addition to this introduction, the Interim NIPP consists of the following chapters:

- Chapter 2—National Goals, Framework, and Actions
- Chapter 3—Vulnerability Reduction Program
- Chapter 4—Threat-Initiated Actions
- Chapter 5—Roles and Responsibilities
- Chapter 6—Integration with Other Plans

The scope and framework of the Interim NIPP are established in Homeland Security Presidential Directive-7 (HSPD-7), "Critical Infrastructure Identification, Prioritization, and Protection," issued in December 2003. HSPD-7 identifies 17 specific CI/KR sectors. Consistent with HSPD-7, the NIPP addresses on-going as well as future activities to be carried out both within these 17 individual CI/KR sectors and nationally across sectors. The Interim NIPP describes DHS leadership of the effort to integrate CI/KR protection activities across sectors.

The Interim NIPP focuses on protection of our Nation's most critical assets within our borders as well as addressing any international linkages. For cyber infrastructures, the United States will work with foreign governments and international organizations to enhance the reliability, availability, and integrity of the Internet. For physical assets located on or near borders with Canada or Mexico, the consequences of an attack may affect the bordering country; protection of the particular asset may require the coordination with or resources from the bordering country. Protection is also necessary when a sector's infrastructure is extensively integrated into an international or global market (e.g., financial services) or when the proper functioning of a sector relies on inputs that are not within our Nation's control. In particular, tampering with or disrupting the flow of critical raw materials into the United States (e.g., by contaminating agricultural products or obstructing transport of energy sources or industrial raw materials), may cause cascading failures within the sector. Therefore, the Interim NIPP includes consideration of these international interdependencies and the vulnerability of assets to threats that originate outside the country.

1.3 Definitions

This section defines key terms used in the Interim NIPP. The term “critical infrastructure” is defined as “systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”[1] “Key resources” are “publicly or privately controlled resources essential to the minimal operations of the economy and government.”[2] “Key assets” (a subset of key resources) are “individual targets whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage our national prestige and confidence.”[3]

Critical infrastructure and key resources are composed of one or more assets. In this document, an asset is something of importance or value and can include one or more of the following types of elements:

- **Human**—The human aspect of an asset includes both the employees to be protected and the personnel who may present an insider threat (e.g., due to privileged access to control systems, operations, and sensitive areas and information).
- **Physical**—The physical aspect may include both tangible property (e.g., facilities, components, real estate, animals, and products) and the intangible (e.g., information).
- **Cyber**—Cyber components include the information hardware, software, data, and networks that serve the functioning and operation of the asset.

The term “sector-specific” agency refers to those Federal departments and agencies identified under HSPD-7 as responsible for the protection activities in specified CI/KR sectors. Exhibit 1 identifies the SSAs and the specific sectors for which they are responsible[4], in coordination with supporting agencies.

Exhibit 1: Sector-Specific Agencies and Assigned Sectors

Department of Agriculture — Agriculture, food (meat, poultry, egg products)

Department of Health and Human Services — Public health and healthcare; Food (other than meat, poultry, egg products)

Environmental Protection Agency — Drinking water and wastewater treatment systems

Department of Energy — Energy, including the production, refining, storage, and distribution of oil and gas, and electric power (except for commercial nuclear power facilities)

Department of the Treasury — Banking and finance

Department of the Interior — National monuments and icons

Department of Defense — Defense industrial base

Department of Homeland Security[5] —

- Information technology
- Telecommunications
- Chemical
- Transportation systems[6]
- Emergency services
- Postal and shipping
- Dams
- Government facilities
- Commercial facilities
- Nuclear reactors, materials, and waste[7]

The terms “protect and secure,” as defined in HSPD-7, mean reducing the vulnerability of CI/KR in order to deter, mitigate, or neutralize terrorist attacks. Thus, as described in this Interim NIPP, critical infrastructure protection includes the activities that identify CI/KR, assess vulnerabilities, prioritize CI/KR, and develop protective programs and measures, because these activities ultimately lead to the implementation of protective strategies to reduce vulnerability.

[1] See USA PATRIOT Act of 2001, 42 U.S.C. § 5195c(e), defining critical infrastructure. This definition is incorporated by reference into the Homeland Security Act of 2002, see 6 U.S.C. § 101.

[2] Homeland Security Act, Section 2(9).

[3] National Strategy for the Physical Protection of Critical Infrastructures and Key Assets” (February 2003), page 7.

[4] Paragraph 18 of HSPD-7 except for Department of Homeland Security.

[5] Paragraph 15 of HSPD-7.

[6] Per Section 22(h) of HSPD-7, DHS and the Department of Transportation will collaborate on all matters relating to transportation security and transportation infrastructure protection.

[7] Under Paragraph 29 of HSDP-7, DHS will work with the Nuclear Regulatory Commission and, as appropriate, DOE in order to ensure the necessary protection of commercial nuclear reactors, research and test nuclear reactors, nuclear materials, and the transportation, storage, and disposal of nuclear materials and waste.

1.4 Key Stakeholders and Partnerships

Although DHS is ultimately accountable for the success of the Nation's CIP program, implementation requires an integrated process across all of the key infrastructure protection stakeholders. These stakeholders include:

- **Department of Homeland Security**—The Department of Homeland Security is the lead agency for the overall national effort to enhance CI/KR protection. In this role, DHS establishes uniform policies and approaches for protection activities, and tracks performance and progress in program implementation. DHS is also the lead agency for the overall assessment of the terrorist threat to the Nation. Building on the efforts of the SSAs, DHS maintains the national inventory of CI/KR assets and carries out national and cross-sector vulnerability assessments, asset prioritization, and, where appropriate, protective measure implementation. DHS also provides specific expertise in addressing the physical, human, and cyber elements of CI/KR, and serves as the lead agency for coordination and information sharing among sector stakeholders.
- **Sector-Specific Agencies**—The SSAs provide the subject matter and industry-specific expertise and relationships to ensure infrastructure protection within the specific sectors. Each SSA is responsible for developing, implementing, and maintaining a Sector-Specific Plan for conducting CIP activities within the sector, which include collaborating with all relevant Federal departments and agencies, State and local governments, and the private sector; identifying assets; conducting or facilitating vulnerability assessments; and encouraging risk management strategies to protect against and mitigate the effects of attacks against CI/KR. While DHS is the SSA for multiple sectors, some organizational elements within DHS have been designated to have primary sector-specific responsibility and are included when referring to SSAs. For example, the Transportation Security Administration (TSA) has this responsibility for the transportation systems sector and the National Cyber Security Division has this responsibility for the information technology sector. The purpose of this designation is to ensure that one organizational element within DHS is the single point of contact and has ultimate accountability for developing the SSP and implementing related CIP activities.

- **Other Federal Agencies**—Federal departments and agencies not designated as SSAs may, nevertheless, provide critical support in the protection of a given sector. Specifically, Federal departments and agencies may provide information on aspects or parts of the sector, or may play a role as the regulatory agency for many owners and operators represented in the sector. Some agencies (e.g., Department of State) may support international outreach to foreign countries or international organizations to strengthen protection of CI/KR.
- **Private Sector**—Because private industry owns and operates the vast majority of the Nation's CI/KR, its involvement is crucial for successful implementation of the NIPP and the national CIP program. Private-sector owners and operators remain the first line of defense for their own facilities and routinely carry out risk management planning and invest in protective measures as a necessary business function. Through various means, the private sector obtains and shares security-related information with Federal, State, and local agencies. As the NIPP is developed and implemented, the specific role of the private sector in the national CIP program (including within each sector) will continue to evolve and be further defined and enhanced.
- **State, Local, and Tribal Entities**—State, local, and tribal entities constitute the front line of response and defense in support of the security spectrum, and may also act as conduits for requests for Federal assistance when the threat exceeds their capabilities. For certain CI/KR, State, local, and tribal entities may serve as owners or

operators of a significant portion of their infrastructure. Furthermore, the Homeland Security Advisor (HSA) in each State serves as the principal point of contact for DHS on homeland security issues. Similar to the private sector, the specific role of State, local, and tribal entities in national CIP will continue to refined and enhanced as the Interim NIPP is implemented.

In order for the national critical infrastructure protection program to be successful, there must be efficient and effective partnership, communication, and coordination among DHS, SSAs, other Federal departments and agencies, private sector owners and operators, and State, local, and tribal entities. The means of partnering with sector stakeholders is evolving as each sector becomes better defined. Prior to the creation of DHS, an architecture of Sector Coordinators and Information Sharing and Analysis Centers (ISACs) was created that began this partnership and achieved early successes. With the creation of DHS and the development of the NIPP, this partnership must evolve to meet new requirements for enhanced capabilities and a revised framework. The NIPP envisions the following three components to implement the public-private partnership:

- **The NIPP Senior Leadership Council**—Will be comprised of the leadership of the Federal departments and agencies engaged in critical infrastructure protection with critical infrastructure owners and operators and State Homeland Security Advisors (HSAs) to lead, integrate, and coordinate the implementation and continuous enhancement of the NIPP through the following activities: advancing collaboration and information sharing within and across sectors, forging consensus on critical infrastructure protection action, evaluating and promoting implementation of risk management-based infrastructure protection programs, and evaluating and reporting on progress. The NIPP Senior Leadership Council is supported by the Cross-Government Coordinating Council and the Cross-Sector Coordinating Council.
- **CI/KR Sector Coordinating Councils**—Are private sector coordinating mechanisms that comprise private sector infrastructure owners and operators and supporting associations, as appropriate. Sector Coordinating Councils bring together the entire range of infrastructure protection activities and issues to a single entity. One role of the Sector Coordinating Councils is to identify or establish and support the information sharing mechanisms (ISMs) that are most effective for their sector, drawing on existing mechanisms (e.g., ISACs) or creating new ones as required.

- **CI/KR Government Coordinating Councils**—Are Government Coordinating Councils for each sector comprised of representatives from DHS, the SSA, and the appropriate supporting Federal departments and agencies. The Government Coordinating Councils work with and support the efforts of the Sector Coordinating Councils to plan, implement and execute sufficient and necessary broad-based sector security, planning and information sharing to support the Nation's homeland security mission.

Chapter 5 of this Interim Plan provides more detailed information on the specific roles and responsibilities of these stakeholders and coordinating mechanisms.

1.5 Next Steps

The national CIP program will be an ongoing effort to protect the Nation's CI/KR. As one of the initial steps in this program, DHS and the SSAs will share and discuss the NIPP framework with the different stakeholders described above to obtain and consider their feedback. Simultaneously, SSAs will work with their stakeholders to begin implementation of the SSPs, so that protective programs and limited resources are targeted at the most critical assets within and across sectors. Success will be achieved by working together through public and private sector partnerships to identify, prioritize, and protect the Nation's CI/KR. Key next steps for different stakeholders include:

- **Private Sector**—The private sector will be engaged by DHS, in collaboration with the relevant SSAs, to promote awareness of and feedback on the NIPP framework and to solicit their involvement in the national CIP program. The private sector will also be working with the appropriate SSAs to begin implementation of the SSPs for their sectors. As the Interim NIPP is implemented, the private sector should expect more coordinated data calls from government agencies, enhanced engagement through Sector Coordinating Councils, and subsequent versions of the NIPP and SSPs will reflect discussions among DHS, the SSAs, and other stakeholders, including the private sector.
- **State, Local, and Tribal Entities**—State, local, and tribal entities will also be engaged by DHS and the SSAs to promote awareness of and provide feedback on the NIPP framework and to solicit their involvement in the national CIP program. The State, local, and tribal entities will also work with the appropriate SSAs to begin implementation of the SSPs for various sectors. As the NIPP is implemented, State, local, and tribal government agencies should expect to experience more coordinated data calls, fewer overlapping efforts to identify and assess critical assets, and subsequent versions of the NIPP and SSPs will reflect discussions between the DHS, the SSAs, and other stakeholders, including State, local, and tribal government agencies.
- **Sector-Specific Agencies**—The SSAs will be key participants in the DHS outreach strategy and have their own dialogue with State, local and tribal entities and the private sector. The SSAs will begin implementing the SSPs, making progress on the initiatives outlined in the SSPs and working with all their respective stakeholders so that SSPs meet the unique challenges of each individual sector. SSAs will utilize, refine, and continue to develop milestones and performance measures to assess progress in each sector. Cross-sector coordination will occur through the NIPP Senior Leadership Council and specific parts of DHS that will be conducting interdependency analyses, developing guidance and tools, and working on a measurement system that provides important feedback to the SSAs.
- **Other Federal Agencies**—Supporting departments and agencies will work with the SSAs to implement the SSPs and participate in sector-specific activities through the Government Coordinating Councils.
- **Department of Homeland Security**—DHS/Information Analysis and Infrastructure Protection (IAIP) Directorate will undertake a major outreach effort to engage all the stakeholders necessary to make the national CIP program a success. In doing so, DHS will work with stakeholders to utilize, refine, and continue to develop milestones and performance measures to assess national-level and sector-by-sector progress. At the same time, it will continue to enhance its programs in information analysis and infrastructure protection and integrate these efforts under the framework of the NIPP.

Appendix N

Interim National Preparedness Goal

Interim
National Preparedness Goal

Homeland Security Presidential Directive 8: *National Preparedness*

Homeland
Security

March 31, 2005

1.0 INTRODUCTION

The terrorist attacks on September 11, 2001, confirmed that all Americans share responsibility for homeland security. Federal, State, local, tribal, private sector, and non-governmental entities and individual citizens across the Nation need to prepare together for major events that will exceed the capabilities of any single entity. The American structure of overlapping Federal, State, local, and tribal levels of governance provides unique opportunities and challenges. Opportunities arise from the flexibility to explore differences, based on unique roles and responsibilities, and share best practices across the Nation. Challenges arise from the need to develop interconnected and complementary national systems that respect those differences and balance flexibility with accountability.

On December 17, 2003, the President issued Homeland Security Presidential Directive 8: *National Preparedness* (see Appendix C). The purpose of HSPD-8 is to "*establish policies to strengthen the preparedness of the United States to prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.*" To prepare as a Nation, HSPD-8 recognizes that, in addition to their direct role in preparedness, government entities must find ways to encourage active participation and involvement of private and non-governmental entities and citizens in national preparedness wherever possible.

HSPD-8 establishes the Secretary of Homeland Security as "*the principal Federal official for coordinating the implementation of all-hazards preparedness in the United States*" and requires establishment of a National Preparedness Goal. "*To help ensure the preparedness of the Nation to prevent, respond to, and recover from threatened and actual domestic terrorist attacks, major disasters, and other emergencies, the Secretary, in coordination with the heads of other appropriate Federal departments and agencies and in consultation with State and local governments shall develop a national domestic all-hazards preparedness goal. …The national preparedness goal will establish measurable readiness priorities and targets that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them. It will also include readiness metrics and elements that support the national preparedness goal including standards for preparedness assessments and strategies, and a system for assessing the Nation's overall preparedness to respond to major events, especially those involving acts of terrorism.*"

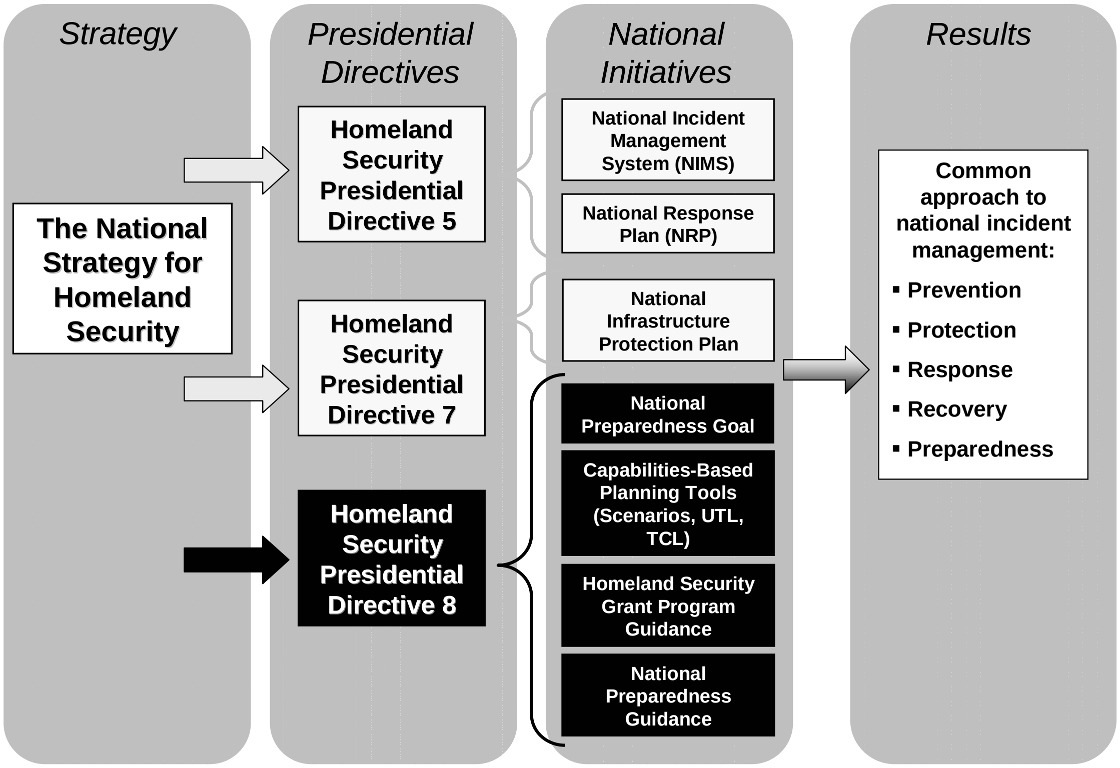
The Secretary of Homeland Security charged the Executive Director of the Office of State and Local Government Coordination and Preparedness (DHS/SLGCP) with responsibility to lead HSPD-8 implementation on his behalf. The National Preparedness Goal (or Goal) is a product of the DHS team, working in coordination with Federal, State, local, tribal, private sector, and non-governmental stakeholders. It provides the means for the Nation to answer three fundamental questions: "*How prepared do we need to be*?", "*How prepared are we*?", and "*How do we prioritize efforts to close the gap*?"

1.1 Relationship to Other Documents

In February 2003, the President issued Homeland Security Presidential Directive 5: *Management of Domestic Incidents* (HSPD-5). HSPD-5 requires DHS to lead a coordinated national effort with other Federal departments and agencies and State, local, and tribal governments to establish a National Response Plan (NRP) and National Incident Management System (NIMS). HSPD-8 is a companion to HSPD-5 (see Figure 1). The Goal will help entities at all levels of government to develop and maintain the capabilities to prevent, respond to, and recover from major events or Incidents of National Significance as described in the NRP and NIMS.

In December 2003, the President issued Homeland Security Presidential Directive: *Critical Infrastructure Identification, Prioritization, and Protection* (HSPD-7). HSPD-7 requires DHS to work closely with other Federal departments and agencies, State and local governments, and the private sector in producing a comprehensive, integrated National Infrastructure Protection Plan (NIPP). The Plan will include coordination and integration, as appropriate, with other Federal emergency management and preparedness activities, including the NRP and applicable national preparedness goals. HSPD-8 supports and complements HSPD-7. The Goal will help entities at all levels of government to develop and maintain the capabilities to identify, prioritize, and protect critical infrastructure and key resources against terrorist attacks as described in the NIPP.

Figure 1: HSPD-8 in Context


Strategy
Presidential Directives
National Initiatives
Results
The National Strategy for Homeland Security
Homeland Security Presidential Directive 5
Homeland Security Presidential Directive 7
Homeland Security Presidential Directive 8
National Incident Management System (NIMS)
National Response Plan (NRP)
National Infrastructure Protection Plan
National Preparedness Goal
Capabilities-Based Planning Tools (Scenarios, UTL, TCL)
Homeland Security Grant Program Guidance
National Preparedness Guidance
Common approach to national incident management:
▪ Prevention
▪ Protection
▪ Response
▪ Recovery
▪ Preparedness

1.2 National Preparedness Defined

HSPD-8 defines preparedness as "*the existence of plans, procedures, policies, training, and equipment necessary at the Federal, State, and local level to maximize the ability to prevent, respond to, and recover from major events. The term 'readiness' is used interchangeably with preparedness*." HSPD-8 refers to preparedness for major events as "*all-hazards preparedness*." It defines major events as "*domestic terrorist attacks, major disasters, and other emergencies*." Major events are synonymous with Incidents of National Significance under the NRP. Incidents of National Significance are defined based on criteria established in HSPD-5 (paragraph 4), as actual or potential high-impact events that require a coordinated and effective response by an appropriate combination of Federal, State, local, tribal, nongovernmental, and/or private sector entities in order to save lives and minimize damage, and provide the basis for long-term community recovery and mitigation activities.

NIMS defines preparedness as *"the range of deliberate, critical tasks and activities necessary to build, sustain and improve the operational capability to prevent, protect against, respond to, and recover from domestic incidents."* The two definitions are complementary. National preparedness involves a continuous cycle of activity to develop the elements (e.g., plans, procedures, policies, training, and equipment) necessary to maximize the capability to prevent, protect against, respond to, and recover from domestic incidents, especially major events that require coordination among an appropriate combination of Federal, State, local, tribal, private sector, and non-governmental entities, in order to minimize the impact on lives, property, and the economy.

1.3 Vision

The National Strategy for Homeland Security (National Strategy), issued in July 2002, states that the Nation must develop "*interconnected and complementary homeland security systems that are reinforcing rather than duplicative and that ensure essential requirements are met*," and "*provide a framework to align the resources of the Federal budget directly to the task of securing the homeland*."

Building upon that strategic intent, the vision for the National Preparedness Goal is:

To engage Federal, State, local, and tribal entities, their private and non-governmental partners, and the general public to achieve and sustain risk-based target levels of capability to prevent, protect against, respond to, and recover from major events in order to minimize the impact on lives, property, and the economy.

1.4 Interim National Preparedness Goal

As required in HSPD-8, the Goal will include readiness targets, priorities, standards for preparedness assessments and strategies, and a system for assessing the Nation's overall level of preparedness. Many of these elements will continue to be updated or refined over time. This document reflects the Department's progress to date to develop each of those elements in coordination with other entities. It will remain in effect until superseded by the Final National Preparedness Goal. The Department will continue to lead an effort with input from Federal, State, local, tribal, private sector, and non-governmental subject-matter experts to define target levels of capability and apportion responsibility for these levels and/or their components among levels of government and groups (or Tiers) of jurisdictions. The Final Goal and a Target Capabilities List (TCL), updated to include the target levels of capabilities, will be issued on October 1, 2005.

2.0 CAPABILITIES-BASED PLANNING TO DEFINE READINESS TARGETS

HSPD-8 states that the National Preparedness Goal will establish *"measurable readiness targets ...that appropriately balance the potential threat and magnitude of terrorist attacks, major disasters, and other emergencies with the resources required to prevent, respond to, and recover from them."* Risk-based target levels of capability will meet that requirement. The intent is to establish capability baselines for operational missions and track resource allocation against them.

It is impossible to maintain the highest level of preparedness for all possibilities all of the time. Managing the risk posed by major events is imperative. Risk-based target levels of capability for major events can be defined through a Capabilities-Based Planning process. Capabilities-Based Planning is defined as planning, under uncertainty, to provide capabilities suitable for a wide range of threats and hazards while working within an economic framework that necessitates prioritization and choice. Capabilities-Based Planning is all-hazards planning. Defining risk-based target levels of capability for the Goal involves identifying a plausible range of major events*;* the tasks to be performed in prevention, protection, response, and recovery that would require a coordinated national effort; and the specific capabilities and levels of capability that would minimize the impact on lives, property, and the economy (see Figure 2).

Appendix O

Recommended Fusion Center Law Enforcement Intelligence Standards

Fusion Center Guidelines

Developing and Sharing Information
and Intelligence in a New World

Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal, and Federal Level

Law Enforcement Intelligence Component

July 2005
Version 1

BJA Bureau of
Justice Assistance

Global Justice Information Sharing Initiative

United States
Department of Justice

Executive Summary

The need to develop and share information and intelligence across all levels has significantly changed over the last few years. The long-standing barriers that built roadblocks among law enforcement agencies, public safety, and the private sector are slowly crumbling. Yet, the need to identify, prevent, monitor, and respond to terrorist and criminal activities remains a significant battle for the law enforcement, intelligence, and public safety communities.

The National Governors Association Center for Best Practices, January 2005 survey reveals that states ranked the development of state intelligence fusion centers as their second highest priority.

Through the support, expertise, and knowledge of law enforcement leaders from all components, the fusion center concept can become a reality. Each official has a stake in the development and exchange of information and intelligence and should act as an ambassador to support and further this initiative. It is the responsibility of leadership to implement and adhere to the fusion center guidelines.

The development and exchange of intelligence is not easy. Sharing this data not only requires strong leadership, it also requires the commitment, dedication, and trust of a diverse group of men and women who believe in the power of collaboration.

How can law enforcement, public safety, and private entities embrace a collaborative process to improve intelligence sharing and, ultimately, increase the ability to detect, prevent, and solve crimes while safeguarding our homeland? Recently, an initiative has emerged that incorporates the elements of an ideal information and intelligence sharing project—fusion centers ("center"). This initiative offers guidelines and tools to assist in the establishment and operation of fusion centers. The guidelines are a *milestone* in achieving a unified force among all levels of law enforcement agencies; public safety agencies, such as fire, health, and transportation; and the private sector. Fusion centers bring all the relevant parties together to maximize the ability to prevent and respond to terrorism and criminal acts. By embracing this concept, these entities will be able to effectively and efficiently safeguard our homeland and maximize anticrime efforts.

What Is the Fusion Center Guidelines Initiative?

As part of the U.S. Department of Justice's (DOJ) Global Justice Information Sharing Initiative (Global), the Criminal Intelligence Coordinating Council (CICC), in support of the Bureau of Justice Assistance, Office of Justice Programs, DOJ efforts to develop fusion center guidelines, recommended the creation of the Intelligence Fusion Center Focus Group.[1] Participants of the focus group included experts and practitioners from local, state, and federal law enforcement agencies as well as representatives from DOJ, the U.S. Department of Homeland

[1] Prior to integrating the public safety and private sector component into this initiative, the workgroup was referred to as the Fusion Center Intelligence Standards Focus Group.

Security (DHS), and the Federal Bureau of Investigation (FBI). In addition, members from national law enforcement organizations and currently operating fusion centers participated in the focus group's efforts. This focus group was tasked with recommending guidelines specifically for the law enforcement *intelligence* component of fusion centers.

In addition, the Homeland Security Advisory Council (HSAC or Council) Intelligence and Information Sharing Working Group has focused on prevention and information sharing by developing guidelines for local and state agencies in relation to the collection, analysis, and dissemination of terrorism-related intelligence in the context of fusion centers. The recommendations resulting from the DOJ initiative and HSAC's efforts lay the foundation for the development of fusion center guidelines for law enforcement intelligence, public safety, and private sector entities.

Through this landmark initiative, it is anticipated that these guidelines will be utilized to ensure fusion centers are established and operated consistently, resulting in enhanced coordination efforts, strengthened partnerships, and improved crime-fighting and antiterrorism capabilities. These guidelines and related materials will provide assistance to centers as they prioritize and address threats posed in their specific jurisdictions for all crime types, including terrorism. In addition, these guidelines will help guide administrators in developing policies, managing resources, and evaluating services.

The development of guidelines for fusion centers has been separated into three phases—law enforcement intelligence, public safety, and the private sector. Fusion center guidelines for the first phase—law enforcement intelligence—are complete. These guidelines may be used for homeland security efforts, as well as all crimes. This report includes an executive summary that contains an overview of the guidelines and their key elements. Also included in this report are additional resources, model policies, and tools for implementation. Guideline development for the second phase—public safety—is currently under way, with plans to incorporate the private sector phase. Integrating these components will not be an easy task. It will take the hard work and dedication of many individuals.

Fusion:

Turning Information and Intelligence Into Actionable Knowledge

What Is the Fusion Process?

The concept of fusion has emerged as the fundamental process to facilitate the sharing of homeland security-related and crime-related information and intelligence. For purposes of this initiative, fusion refers to the overarching process of managing the flow of information and intelligence across levels and sectors of government. It goes beyond establishing an intelligence center or creating a computer network. The fusion process supports the implementation of risk-based, information-driven prevention, response, and consequence management programs. At the same time, it supports efforts to address immediate and/or emerging threat-related circumstances and events. Data fusion blends data from different sources, including law enforcement, public safety, and the private sector, resulting in meaningful and actionable intelligence and information. The fusion process also allows for relentless reevaluation of existing data in context with new data in order to provide constant updates. The fusion process turns information and intelligence into actionable knowledge.

What Is a Fusion Center?

A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources. In addition, fusion centers are a conduit for implementing portions of the *National Criminal Intelligence Sharing Plan* (NCISP or Plan). The NCISP is regarded as the blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. The Plan contains over 25 recommendations that were vetted by law enforcement officials and experts from local, state, tribal, and federal agencies. The Plan embraces intelligence-led policing, community policing, and collaboration, and it serves as the foundation for the fusion center intelligence guidelines.

For the purposes of this initiative, **a fusion center is defined as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.** The intelligence component of a fusion center focuses on the intelligence process, where information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity.

The principal role of the fusion center is to compile, blend, analyze, and disseminate criminal intelligence and other information (including but not limited to threat assessment, public safety, law enforcement, public health, social service, and public works) to support efforts to anticipate, identify, prevent, and/or monitor criminal activity.

The fusion process involves every level and sector (discipline) of government, private sector entities, and the public—though the level of involvement of some of these participants will vary based on specific circumstances. For purposes of this report, the fusion process should be organized and coordinated on a statewide level, and each state should establish and maintain a center to facilitate the fusion process.

Although each fusion center will have unique characteristics, it is important for centers to operate under a consistent framework—similar to the construction of a building where each structure is unique, yet a consistent set of building codes and regulations are adhered to regardless of the size or shape of the building.

Why Should Fusion Centers Be Established?

The ultimate goal is to provide a mechanism where law enforcement, public safety, and the private sector can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity. As funds continue to be stretched to support numerous initiatives, it will be critical for government to accomplish ***more with less***. Fusion centers embody the core of collaboration, and as demands increase and resources decrease, fusion centers will become an effective tool to maximize available resources and build trusted relationships**.**

It is recommended that fusion centers adhere to these guidelines and integrate the key elements of each guideline to the fullest extent.

Appendix P

2005 National Capital Region Homeland Security Strategic Plan

2005 National Capital Region Homeland Security Strategic Plan

“A Strategic Partnership to Manage Risk”

2005 NCR-HLS Strategic Plan

Guiding Principles, Vision, Mission, Strategic Goals & Objectives

Introduction

The National Capital Region (NCR) encompasses a unique group of jurisdictions with a diverse set of needs and interests. The NCR is home to infrastructure that is both critical and symbolic to our nation. This presents the homeland security leadership of these jurisdictions with a unique risk that can only be effectively managed through an integrated and collaborative effort.

This is the strategic plan for the National Capital Region Homeland Security Partners and is intended as a guiding framework for a safe and secure NCR. The NCR Homeland Security Partnership is comprised of the region's local, state, regional, and federal governments, citizen community groups, private sector, non-profit organizations, and non-governmental organizations.

> *"We must calibrate an approach to security that incorporates prevention*
> *and protection into our lives in a way that respects our liberty*
> *and our privacy, and fosters our prosperity."*

~Secretary Michael Chertoff,
March 16, 2005 Remarks, George Washington
University Homeland Security Policy Institute

Vision

The Vision for the NCR Homeland Security Partners is…

Working together towards a safe and secure National Capital Region.

Mission

The Mission Statement for the NCR Homeland Security Partners is to…

Build and sustain an integrated effort to prepare for, prevent, protect against, respond to, and recover from "all-hazards" threats or events.

“**NCR Homeland Security Partners**" refers to the region’s local, state, regional, and federal governments, citizen community groups, private sector, non-profit organizations, and non-governmental organizations.

A "**best-practice**" approach draws from actual experience and lessons learned. A "**performance-based**" approach is outcome focused and can be evaluated using scenarios.

“All-hazards” preparedness refers to preparedness for domestic terrorist attacks, major disasters, and other emergencies. (Source: *Homeland Security Presidential Directive/HSPD-8*, December 2003)

Guiding Principles

1. *Strengthen regional coordination among all partners to gain synergy while sustaining jurisdictional authority and enhancing capabilities.*
2. *Implement homeland security policies and programs while maintaining our constitutionally-based society, particularly the civil rights and civil liberties of the NCR’s diverse population, including persons with disabilities.*
3. *Prepare for “all-hazards”, including man-made and naturally occurring emergencies and disasters.*
4. *Advance the safety and security of the NCR in ways that are enduring, relevant, and sustainable.*
5. *Foster a culture of collaboration, respect, communication, innovation, and mutual aid among all homeland security partners across the NCR.*
6. *Adopt best-practice, performance-based approaches to staffing, planning, equipping, training, and exercising for all homeland security partners.*
7. *Strive for an optimal balance of preparedness capabilities across the NCR that recognizes differing risks and circumstances, and leverages mutual aid agreements.*

Strategic Goals

1. ***Planning & Decision-Making:*** A collaborative culture for planning, decision-making, and implementation across the NCR.

2. ***Community Engagement:*** An informed and prepared community of those who live, work, and visit within the region, engaged in the safety and security of the NCR.

3. ***Prevention & Mitigation:*** An enduring capability to protect the NCR by preventing or mitigating "all-hazards" threats or events.

4. ***Response & Recovery:*** A sustained capacity to respond to and recover from "all-hazards" events across the NCR.

Strategic Goal 1

A collaborative culture for planning, decision-making, and implementation across the NCR.

Objectives

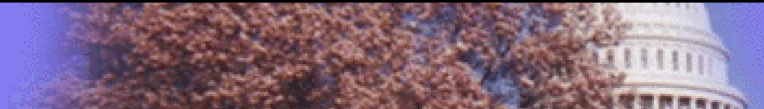
- Enhance and continually adapt the framework for regional strategic planning and decision-making to achieve an optimal balance of capabilities across the NCR.
- Design and implement an integrated and iterative performance and risk-based regional planning process that engages appropriate NCR homeland security partners.
- Establish an NCR-wide assessment process to identify and remedy gaps in regional, jurisdictional, and sector preparedness.
- Develop a requirements generation and prioritization process to effectively utilize available public and private homeland security resources to satisfy NCR regional, jurisdictional, and sector preparedness.
- Enhance the oversight and accountability process that coordinates, tracks, and evaluates the implementation and effectiveness of regional decisions.
- Adopt a lifecycle cost and investment approach to generate enduring and sustainable preparedness across the NCR.

Strategic Goal 2

An informed and prepared community of those who live, work, and visit within the region, engaged in the safety and security of the NCR.

Objectives

- Deliver timely, coordinated and targeted emergency information across the NCR before, during, and after emergencies.
- Raise the level of preparedness across the NCR by utilizing and enhancing public awareness and education campaigns.
- Strengthen public-private-NGO partnerships and communications through increased sharing of information and resources, and expanded participation in preparedness planning across the NCR.
- Engage those who live, work and visit within the region in emergency preparedness across the NCR.



Strategic Goal 3

An enduring capability to protect the NCR by preventing or mitigating “all-hazards” threats or events.

Objectives

- Develop and sustain common, multi-disciplinary standards for planning, equipping, training, operating, and (cross-jurisdictional) exercising to maximize prevention and mitigation capabilities across the NCR.
- Strengthen the gathering, fusion, analysis, and exchange of multi-discipline strategic and tactical information and data for shared situational awareness.
- Employ a performance- and risk-based approach to critical infrastructure protection across the NCR, targeting resources where the threat, vulnerability, and impact are greatest.

Strategic Goal 4

A sustained capacity to respond to and recover from “all-hazards” events across the NCR.

Objectives

- Develop, adopt, and implement integrated plans, policies, and standards to facilitate response and recovery.
- Ensure the capacity to operate multi-level coordinated response and recovery.
- Ensure adequate and effective sharing of resources.
- Comprehensively identify long-term recovery issues.